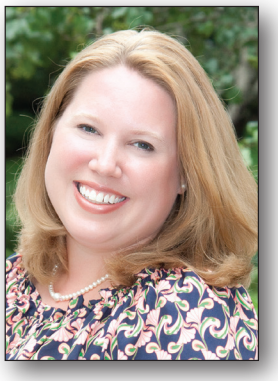
PATTISHALL insights

Join us on LinkedIn https://www.linkedin.com/company/pattishall-mcauliffe

APRIL 2016

> "FIRMS NOW USE THE CFAA TO PROTECT THEIR OWN ELECTRONICALLY STORED INFORMATION AGAINST HACKING AND MISUSE OF DATA."



Computer Fraud and Abuse Depends on Where You Are, Not Just What You Did

By Ashly Boesche

In 2015, there were more than three billion Internet users.[1] With the increase of online traffic and more and more people relying on the Internet for everyday activities, from online shopping, banking, and managing their health, hacking has been on the rise.[2] Hackers have stolen highly sensitive personal, financial, and health information affecting millions of people.[3] Hackers have demonstrated that no one is immune, attacking not only major retailers such as Target, eBay, and Home Depot, but also attacking the United States federal government. Globally, the cost of cybercrimes is over a trillion dollars. Businesses and individuals alike suffer the consequences of these crimes.

To combat the rise of cyber-attacks, Congress passed the Computer Fraud and Abuse Act ("CFAA") in 1984. When the CFAA was enacted, its primary aim was against threats to national security, limiting protection to "federal interest computers." However, with the increasing amount of personal data stored electronically, the scope of the CFAA has expanded.[4]

Firms now use the CFAA to protect their own electronically stored information against hacking and misuse of data. Most commonly, private business owners have alleged violations of 18 U.S.C. § 1030(a)(2), which applies when one "[i]ntentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information contained in a financial record, information from any department or agency of the United States, or information from a protected computer." Although the CFAA defines "exceeds authorized access" as "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter,"[5] what constitutes "without authorization" has been left undefined.

The federal courts have differed in their interpretations of the meaning of "exceeds authorized access," creating a circuit split. The Second, Fourth, and Ninth Circuits[6] have adopted a narrow approach, finding CFAA violations only when data is accessed through hacking. The First, Fifth, Seventh, Eighth, and Eleventh Circuits[7] have adopted a much broader view, finding CFAA violations in data misuse, even when an individual has lawful access to the data. Recent cases demonstrate the drastically different outcomes of CFAA claims.

1. *Internet Live Stats,* March 30, 2015 (http://www.internetlivestats.com/internet-users/)
2. Hacking includes breaking passwords, creating logic bombs, denial of service attacks; writing and releasing viruses and worms, viewing restricted, electronically-stored information owned by others; URL redirection; adulterating web sites; or any other behavior that involves accessing a computer system without appropriate authorization. Peter T. Leeson & Christopher J. Coyne, *The Economics of Computer Hacking*, 1 J.L. ECON & POL'Y, 511, 514 (2005).
3. Julie Hirschfeld Davis, *Hacking of Government Computers Exposed 21.5 Million People*, N.Y. TIMES (July 9, 2015), http://www.nytimes.com/2015/07/10/us/office-of-personnel-management-hackers-got-data-of-millions.html?_r=0.
4. In 1994, the CFAA was amended to permit civil actions. In 1996, the CFAA was again amended to substitute "federal interest computer" with "protected computer."
5. 18 U.S.C. § 1030(e)(6).
6. *See U.S. v. Valle*, 807 F.3d 508 (2nd Cir. 2015); *WEC Carolina Energy Solutions v. Miller*, 687 F.3d 199 (4th Cir. 2012); and *LVRC Holdings, LLC v. Brekka,* 581 F.3d 1127 (9th Cir. 2009).
7. *See EF Cultural Travel BV v. Zefer Corp.*, 318 F.3d 58 (1st Cir. 2003); *United States v. Musacchio*, 590 Fed. Appx. 359 (5th Cir. 2014); *Int'l Airport Ctrs. v. Citrin*, 440 F.3d 418 (7th Cir. 2006); *United States v. Teague*, 646 F.3d 1119 (8th Cir. 2011); and *United States v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010).

> “IN THE ABSENCE OF CONGRESSIONAL OR SUPREME COURT INTERVENTION, OUTCOMES OF CFAA CASES WILL CONTINUE TO DIVERGE, DEPENDING UPON THE LAW OF THE APPLICABLE CIRCUIT.”

For example, in *United States vs. Nosal*, 676 F.3d 854 (9th Cir. 2012), Nosal, an employee at an executive search firm, left to start a competing business and subsequently recruited former colleagues to join him. Before their departure, the former colleagues used their company log-in credentials to access information from the confidential database and shared the data with Nosal. The Ninth Circuit found that because the employees were authorized to access the information, they did not violate the CFAA unless and until that authorization was revoked. The Ninth Circuit reasoned that without the revocation of authorization, employees would not have notice of when their acts may be criminal. The Ninth Circuit also cautioned that a broader reading of the CFAA would transform the anti-hacking statute into an expansive misappropriation statute. Ultimately, the Ninth Circuit held that “exceeds authorized access” under the CFAA is limited to violations of restrictions to access to information, and not restrictions of its use.

In direct contrast to this narrow approach, the First, Fifth, Seventh, Eighth, and Eleventh Circuits have adopted a much broader analysis, which encompasses the misuse of information and violations of an employer’s policy. For example, in *Int’l Airport Centers v. Citrin*, 440 F. 3d 418 (7th Cir. 2006), the plaintiff, International Airport Centers, provided the defendant, Citrin, with a laptop to use for work purposes. Citrin’s primary responsibility was to collect data for targets. Citrin quit and deleted all of the data stored on the laptop. International Airport Centers sued Citrin alleging that he violated the CFAA because his authorized access to the laptop ceased when he quit. In reversing the district court’s dismissal of International Airport Centers’ case, the Seventh Circuit, relying on agency principles, found that Citrin’s authorization was revoked when he violated his employment contract. Therefore, Citrin could be found to violate the CFAA.

The circuit divide continues. In December 2015, the Second Circuit recently joined the First, Fifth, Seventh, Eighth, and Eleventh Circuits, adopting the broad interpretation in *United States v. Valle*, 807 F.3d 508 (2d Cir. 2015). The Tenth Circuit is currently considering a case which applies the narrow approach.[8]

In an effort to address the CFAA’s vagueness and the circuit split, the Senate introduced Aaron’s Law in 2013. Aaron’s Law seeks to replace “exceeds authorized access” with “access without authorization,” which is defined as “obtaining information on a protected computer that the accesser lacks authorization to obtain by knowingly circumventing one or more technological or physical measures that are designed to exclude or prevent unauthorized individuals from obtaining that information.” This proposed legislation therefore supports adopting the narrow approach which requires hacking. The legislation was re-introduced to the House and Senate on April 21, 2015 and referred to the House Committee on the Judiciary on May 15, 2015, but has yet to be enacted into law.[9]

With the state of the law of the CFAA in flux, it is critical that individuals and businesses alike take steps to protect data. Some practical tips that private firms may use to protect their data include implementing strong firewalls, conducting security audits, reviewing security logs for unusual activity, encrypting data, restricting administrative access on workstations, restricting write-access to removable drives to avoid data leakage, implementing application whitelisting, creating and following data retention plans and policies and conducting periodic security awareness training. In the absence of Congressional or Supreme Court intervention, outcomes of CFAA cases will continue to diverge, depending upon the law of the applicable circuit. ■

8. *Tank Connection, LLC v. Haight*, No. 6:13-CV-01392-JTM, 2016 WL 492751 (D. Kan. Feb. 8, 2016).
9. *See* Aaron’s Law Act of 2015, available at https://www.congress.gov/bill/114th-congress/senate-bill/1030.

*firm*UPDATE

APPOINTMENTS

Phillip Barengolts

Phil has been appointed to the INTA North American Global Advisory Council for 2016-2017.

Thad Chaloemtiarana

Thad has been nominated to serve as Membership Officer for the ABA Section of Intellectual Property Law for 2016-2017.

Robert W. Sacoff

Bob has been appointed to the AIPPI Standing Committee on Geographical Indications, and to the Working Committee preparing the US Group report on "Linking and Making Available on the Internet," which is on the agenda for the 2016 World Congress in Milan in September.

PRESENTATIONS

Jessica A. Ekhoff

Jessica will speak at The Science Fiction & Fantasy Writers of America 50th Anniversary Nebula Conference on "All's Clear - Or Is It? Titles, Character Names, Set Design, and Other Clearance Issues for Authors and Filmmakers" on May 13, in Chicago.

Jonathan S. Jennings

Jonathan spoke on social media and identity rights issues at The John Marshall Law School's 60th Annual Intellectual Property Law Conference in Chicago on February 26.

Janet A. Marvel

Janet will appear at the Lexis Nexis booth at INTA on May 10 to discuss her co-authored "*Trademarks and Unfair Competition Deskbook*," now in its 7th Edition.

Belinda J. Scrimenti

Belinda will moderate a Table Topic on "The TTAB and Genericness - Are Recent Rulings an Evolution or Revolution?" at the INTA Annual Meeting in Orlando on May 25.

Joseph N. Welch II

Joe presented an "Overview of 2015-16 Federal Court, TTAB and UDRP Decisions," at the Practising Law Institute's Advanced Trademark Law Annual Review in New York City on March 22.

Uli Widmaier

Uli moderated the panel on "Litigating Trade Dress and Functionality Cases" and spoke on "Trade Dress and Functionality" at the ABA's 31st Annual Intellectual Property Law Conference in Bethesda, MD, on April 7. In addition, Uli co-presented a 90-minute webinar on "Trademark Infringement: Demonstrating Irreparable Harm to Obtain an Injunction" for Strafford Publications, Inc. on April 21.

PUBLICATIONS

Seth I. Appel

Seth's case note, "First Amendment Protects Registration of Disparaging Trademarks, Federal Appellate Court Holds," was published in the March edition of *AIPPI e-News*.

Ashly Boesche

Ashly co-authored an article entitled "Judge James Holderman, U.S. District Court, Northern District of Illinois (Retired), In His Own Words: IP Litigation Strategy Advice and Insight," in the March/April 2016 Issue of *Landslide* Magazine.

David C. Hilliard, Joseph N. Welch II, Uli Widmaier

The Eleventh Edition of Hilliard, Welch and Widmaier, *Trademarks and Unfair Competition*, will be published in June (2016, Carolina Academic Press), a text book used in over fifty law school courses nationally.

Jonathan S. Jennings and Kristine A. Bergman

Jonathan co-authored the 2016 edition of the treatise entitled "*Trademarks and Unfair Competition: Critical Issues in the Law,*" published by The Law Journal Press of New York. In addition, he authored the updated Illinois chapter of INTA's *U.S. State Trademark and Unfair Competition Law* with Kristine's assistance.

Uli Widmaier and Kristine A. Bergman

Uli and Kristine conducted an interview with Professor Mark Lemley of Stanford Law School on "Reining in Right of Publicity," which was published in the March/April 2016 edition of *Landslide* Magazine.

TEACHING

Ashly Boesche

Ashly is teaching Trademark Law and Unfair Competition at Chicago-Kent College of Law.

Uli Widmaier

From January through March, Uli co-taught the seminar on "Advanced Trademarks and Unfair Competition" at the University of Chicago Law School. This marks the 14th year that Uli has taught this seminar.

firm NOTEWORTHY

Brett A. August

Brett been named 2016 "Brand Protection Attorney of the Year in Illinois" by *Corporate INTL* Magazine. He was also featured in "The French Connection," in the 2016 issue of *Illinois Super Lawyers* Magazine, detailing how he became a Chevalier de la Légion d'Honneur for enhancing relations between Paris and Chicago.

Ashly Boesche

Ashly coached the victorious 2016 IIT Chicago-Kent College of Law moot court team to its first place and best brief awards in the Saul Lefkowitz Midwest Regional Trademark Competition on February 6. The team, under Ashly's tutelage, then proceeded to finish second place in national overall performance, brief and oral argument in the National Championship at the U.S. Court of Appeals for the Federal Circuit on March 12. No other team placed in all three categories.

Pattishall Medal for Teaching Excellence

INTA has announced that the 2016 Pattishall Medal will be awarded in July, and the recipient will be introduced at the Leadership Meeting in November. The Medal recognizes teaching excellence in the trademark, trade identity and unfair competition field. Nominations are being accepted at www.inta.org/pattishall until April 29. Email pattishall@inta.org with any questions.

PATTISHALL
MCAULIFFE
NEWBURY
HILLIARD &
GERALDSON LLP

200 South Wacker Dr.
Suite 2900
Chicago IL 60606-5896

312.554.8000 | pattishall.com | twitter.com/pattishall