No. 19-783

IN THE

Supreme Court of the United States

NATHAN VAN BUREN,

Petitioner,

v.

UNITED STATES,

Respondent.

ON WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE ELEVENTH CIRCUIT

BRIEF FOR *AMICUS CURIAE* UNITED STATES TECHNOLOGY POLICY COMMITTEE OF THE ACM IN SUPPORT OF NEITHER PARTY

ARNON D. SIEGEL, ESQ.
655 Avenue of the Americas
New York, New York 10010

ANDREW GROSSO
Counsel of Record
MARK D. RASCH
RONALD J. JARVIS
ANDREW GROSSO & ASSOCIATES
1101 Thirtieth Street NW,
Suite 500
Washington, D.C. 20007
(202) 298-6500
agrosso@acm.org

Counsel for Amicus Curiae

297053

COUNSEL PRESS
(800) 274-3321 • (800) 359-6859

TABLE OF CONTENTS

Page

TABLE OF CONTENTS. i

TABLE OF AUTHORITIES ii

INTEREST OF THE AMICUS CURIAE 1

SUMMARY OF THE ARGUMENT. 2

ARGUMENT. 3

THE DEFINITION OF "EXCEEDING UNAUTHORIZED ACCESS" CANNOT BE INTERPRETED TO INCLUDE ACCESSING DATA PUBLICLY DISCLOSED ON THE INTERNET 3

A. The CFAA Must Be Construed Narrowly. 4

B. Publishing Information on the Internet Grants Authority to Access That Information 5

C. The Automated Scraping of the Internet for Publicly Posted Data, for Whatever Purpose, Is Not Prohibited by the CFAA 9

D. Automated Scraping Is an Invaluable Tool for Information Technology Professionals. 12

CONCLUSION 20

APPENDIX. 1a

TABLE OF CITED AUTHORITIES

Page

Cases

Facebook, Inc. v. Power Ventures, Inc.,
844 F.3d 1058 (9th Cir. 2016). 6

HiQ Labs, Inc. v. LinkedIn Corp.,
938 F.3d 985 (9th Cir. 2019). 7

Jones v. United States,
529 U.S. 848 (2000) 4

Leocal v. Ashcroft,
543 U.S. 1 (2004). 4

QVC, Inc. v. Resultly, LLC,
159 F. Supp. 3d 576 (E.D. Pa. 2016) 7

Sandvig v. Barr,
2020 U.S. Dist. LEXIS 53631
(D.D.C. March 27, 2020) 9

United States v. John,
597 F.3d 263 (5th Cir. 2010). 6

United States v. Morrison,
844 F.2d 1057 (4th Cir. 1988). 12

United States v. Nosal,
676 F.3d 854 (9th Cir. 2011). 8

Page

United States v. Thompson/Center Arms Co.,
504 U.S. 505 (1992) 5

United States v. Valle,
807 F.3d 508 (2d Cir. 2015) 5

United States v. Wiltberger,
18 U.S. (5 Wheat.) 76 (1820) 4

Yates v. United States,
574 U.S. 516 (2015) 4

Statutes and Other Authorities

17 U.S.C. § 506(a)(B) 12

17 U.S.C. § 506(a)(C) 12

17 U.S.C. § 1201 11

18 U.S.C. § 641 12

18 U.S.C. § 1029 11

18 U.S.C. § 1030(a)(2) 3

18 U.S.C. § 1030(a)(2)(B) 12

18 U.S.C. § 1030(a)(2)(C) . . . . . *passim*

Cited Authorities

Page

18 U.S.C. § 1030(a)(5)(A) 10

18 U.S.C. § 1030(e)(6) 8

18 U.S.C. § 1030(g) 11

18 U.S.C. § 1343 11

18 U.S.C. § 1831 11

18 U.S.C. § 2701 11

Simson Garfinkel & Gene Spafford, Web Security, Privacy and Commerce (2d ed. 2011) 6

INTEREST OF THE AMICUS CURIAE

The United States Technology Policy Committee ("USTPC") is the U.S. public policy committee of the Association for Computing Machinery ("ACM"). ACM is the oldest and largest international scientific and educational organization in the field of computing, with a membership of over 100,000 professionals. It is dedicated to advancing the arts, sciences, and applications of information technology. USTPC educates U.S. government organizations, the computing community, and the American public on matters of U.S. public policy concerning information technology.

USTPC submits[1] this brief *amicus curiae* out of a firm conviction that the questions posed in this case affect in pivotal ways data and computing scientists, as well as other professionals who make use of the Internet and computing technology. Increased reliance upon the use of the Internet in all professions makes it critical that clear, bright, and unambiguous lines be drawn as to what the laws do and do not proscribe. Such clarity is particularly important when the underlying technology and the ubiquitous use of that technology continue to change at a rapid and accelerating pace, and where the laws to be clarified include criminal as well as civil liability for their breach. The members of the USTPC on this brief are listed in the appendix.

---

1. No counsel for a party authored this brief in whole or in part, and no such counsel or party made a monetary contribution intended to fund the preparation or submission of this brief. No person other than amici curiae, their members, or their counsel made a monetary contribution to its preparation or submission. The parties have consented to the filing of this brief.

SUMMARY OF THE ARGUMENT

Section 1030(a)(2)(C) of the Computer Fraud and Abuse Act ("CFAA") proscribes "exceeding authorization" when accessing a computer and thereby obtaining information. This statute is both criminal and civil. Moreover, it is capable of both a broad reading, proscribing any use of any kind of electronic device in any manner and for any purpose not expressly permitted by the device's owner—essentially using the CFAA to furnish civil, contractual prohibitions with criminal penalties; or a narrow reading, interpreting the Section as akin to a "data theft statute"—thereby restricting this provision of the statute to the proscription actually set forth in its text.

The USTPC represents information technology professionals, including data scientists, who use computer systems and the Internet to conduct research and to learn about society and the world. These professionals, along with security researchers, innovators, and those who test, prod, and probe the connections between and among systems functioning on the Internet, must remain free to find, collect, and use publicly-available data, and to access the publicly-available systems on which data are maintained, without the threat of prosecution or civil lawsuit. The CFAA must be read narrowly, according to its stated terms as drafted by Congress, allowing free access to publicly available information.

ARGUMENT

THE DEFINITION OF "EXCEEDING UNAUTHORIZED ACCESS" CANNOT BE INTERPRETED TO INCLUDE ACCESSING DATA PUBLICLY DISCLOSED ON THE INTERNET

Section 1030(a)(2) of the CFAA prohibits a person from intentionally "access[ing] a computer without authorization," or doing so while intentionally "exceed[ing] authorized access," and thereby "obtaining information from any protected computer." 18 U.S.C. § 1030(a)(2)(C).

A "protected computer" includes any computer operating in interstate commerce. 18 U.S.C. § 1030(e)(2)(B). This definition includes any computer connected to the Internet—which today is almost every computer. Therefore, the information protected by Section 1030(a)(2)(C) includes all websites that are maintained on such computers and all the information on those websites.

The Court and the Petitioner have framed the issue here as follows (emphasis added):

> Whether a person who is authorized to access information on a computer for certain purposes violates Section 1030(a)(2) of the Computer Fraud and Abuse Act if he accesses the same information *for an improper purpose*.

This framing raises, indeed it *begs*, two questions: *first*, what *is* an "improper purpose"; and, *second*, what does a person's "purpose" for accessing information *have to do* with the prohibitions in the Act, if anything.

"Proper" and "improper" purposes are neither defined nor otherwise referenced by the Act.

These questions are significant because of the usual way that the Internet operates: by posting information (*i.e.*, webpages and their contents, without password protections, copyright protection, or other control devices), the information is publicly disclosed—it is made available to the public for anyone to access. Thereafter any attempt to limit access to that information results in an inherent contradiction: by making the information available in this manner to the public, the posting entity has given access to the information to the world; so how can access by any particular person, or access for any particular purpose, exceed the authorization that was initially given?

The answer is that it cannot.

A. The CFAA Must Be Construed Narrowly

The CFAA imposes both civil and criminal liability. For this reason, the rule of lenity applies;[2] and the prohibitions in the Act, whether in the criminal or civil context, must be interpreted similarly. *See Leocal v. Ashcroft*, 543 U.S. 1, 11 n.8 (2004).

---

2. The rule of lenity requires "penal laws . . . to be construed strictly." *United States v. Wiltberger*, 18 U.S. (5 Wheat.) 76, 95 (1820). "[W]hen choice has to be made between two readings of what conduct Congress has made a crime, it is appropriate, before we choose the harsher alternative, to require that Congress should have spoken in language that is clear and definite." *Jones v. United States*, 529 U.S. 848, 858 (2000) (internal quotation marks and citation omitted); *see also Yates v. United States*, 574 U.S. 516, 547-48 (2015) (application of the rule of lenity ensures that criminal statutes will provide fair warning concerning conduct rendered illegal.)

Because it is a criminal law, the CFAA must be narrowly construed—even in the civil context. Questions as to the conduct proscribed, including the scope of safe harbors, must be resolved in favor of a defendant. *Id.* (citing *United States v. Thompson/Center Arms Co.*, 504 U.S. 505, 517-18 (1992) (plurality opinion) (applying the rule of lenity to a tax statute, in a civil setting, because the statute had criminal applications and thus had to be interpreted consistently with its criminal applications)). *See generally United States v. Valle*, 807 F.3d 508, 523 (2d Cir. 2015) (discussing application of the rule of lenity in reversing conviction under the Computer Fraud and Abuse Act).

B. Publishing Information on the Internet Grants Authority to Access That Information

The act of publicly posting information on the Internet, by its nature, authorizes a user of the Internet to view that data, *viz.*, to access it.

At a high level, here is how web pages and readers on the Internet interact: (1) a webpage is placed on or "hosted" (maintained) by a computer, or "server," operated by the person posting that webpage; (2) a viewer (doing so electronically, through his or her web browser on his or her own computer) makes a request of the server hosting the webpage to send to his or her computer a copy of the data on that web page;[3] (3) the server responds by transmitting

3. At this point, there is an intermediate step: the server, acting on the instructions with which it has been programmed, determines what information to release to the viewer. This may be as simple as providing all of the information on an entire web page; or may involve creating custom content for only that viewer;

a copy of the webpage and possibly additional data to the viewer's computer; and (4) the viewer's computer then reconstructs the webpage for the viewer to examine. *See generally* SIMSON GARFINKEL & GENE SPAFFORD, WEB SECURITY, PRIVACY AND COMMERCE (2d ed. 2011). In effect, the poster authorizes the viewer to request, download, copy, and take possession of the data in its entirety.

Technologically, the question of motive or purpose does not arise. *Nor does it arise under the CFAA*.

As noted above, Section 1030(a)(2)(C) of the CFAA prohibits a person from intentionally "access[ing] a computer without authorization," or doing so while intentionally "exceed[ing] authorized access," and thereby "obtaining information." Nowhere is "motive," "goal," "reason," or "purpose," whether proper or improper, mentioned—it is not in this Section. Because this is a criminal law, and must be narrowly construed, it cannot be *read into* the Section.

Violations of terms of service, policy statements, warning notices, and the like do not convert the accessing of information into "exceeding" the authorization already granted to access that information. This is so because the authority to view, download, and copy the data was granted *in toto* by the public posting of the data. There is no other authorization required. *See, e.g.*, *Facebook, Inc. v. Power Ventures, Inc.*, 844 F.3d 1058, 1067 (9th Cir. 2016) ("[A] violation of the terms of use of a website—without more—cannot establish liability under the CFAA."). *Contra United States v. John*, 597 F.3d 263, 273 (5th Cir.

---

or the server may refuse to respond to a request that it deems to be unauthorized.

2010) (employee who accesses information from a company computer, which information he is entitled to access, exceeds his authority to access such information when he does so both in violation of company policy and for use in a criminally fraudulent scheme).

As the Ninth Circuit noted in *HiQ Labs, Inc. v. LinkedIn Corp.*, 938 F.3d 985, 1002 (9th Cir. 2019), *petition for cert. filed*, No. 19A819 (2020):

> [T]he CFAA contemplates the existence of three kinds of computer information: (1) information for which access is open to the general public and permission is not required, (2) information for which authorization is required and has been given, and (3) information for which authorization is required but has not been given (or, in the case of the prohibition on exceeding authorized access, has not been given for the part of the system accessed).[4]

This is not to say that the clause regarding "exceeding authorized access" has no meaning. Nor does it imply that there are not other statutes that address improper motive

4. However, an Internet user must not have to *guess* whether he or she has authority to access information on a computer system, nor be subject to a risk that he or she is *mistaken* in this regard. Unless a prohibition is clear and unambiguous, the authority must be deemed granted. *Cf. QVC, Inc. v. Resultly, LLC*, 159 F. Supp. 3d 576, 596 (E.D. Pa. 2016) ("The relevant question is not whether [the defendant] Resultly was granted permission to access the information on [the website] QVC.com, but whether that authorization was ever rescinded or limited in a way that would put Resultly on notice that it was not authorized to access information it was otherwise entitled to access.").

or improper conduct—it is simply that Section 1030(a)(2)(C) does not, and must not be read as prohibiting access with any particular motive or by any particular means.

"Exceeding authorized access" has a meaning. The CFAA defines the term "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." 18 U.S.C. § 1030(e)(6). (We confine ourselves here to the prong of "obtaining" information, as the alteration of information in a computer in not at issue in this case.)

As noted above, the posting of information on the Internet by means of maintaining it on a computer that is connected to the Internet means, by necessity, allowing anyone who can view that information to have full access to it. "Exceeding authorized access" in such a context is not possible.

With this being said, this prong of the statute does have a meaning: when a person who has authority to access a computer system generally does so, but then *hacks* into a portion of the system that he or she is not permitted to access. *See United States v. Nosal*, 676 F.3d 854 (9th Cir. 2011) (*en banc*) (discussing hacking in the context of the CFAA). However, because *motive* is not mentioned in this Section of the CFAA, it must not be read into this Section so as to expand the conduct proscribed by Congress. Similarly, the Section does not mention the *means* whereby a user accesses the information: it mentions neither browsing and viewing by an individual; nor the use of automated software (colloquially known as

a "bot") to mechanically examine and collect, or "scrape,"[5] all or a sizeable portion of a website.[6]

C. The Automated Scraping of the Internet for Publicly Posted Data, for Whatever Purpose, Is Not Prohibited by the CFAA

Data researchers have many reasons for collecting and analyzing information available on the Internet. Examples of these reasons include: the evaluation of gender and racial biases on the Internet for job postings and other employment matters, and for the award of contracts, grants, and similar economic advantages; the correlation of financial grants and contributions to authors of published articles, so as to identify possible conflicts of interest affecting the reliability of the analysis and conclusions in those articles; the evaluation and comparisons of economic data of categories of individuals, of companies, of nations, etc.; the mapping of geographic data; and audits of search engine functions for accuracy, biases, and conflicts of interest. Concrete examples of these and other research projects are set out below for the Court's consideration.

Section 1030(a)(2)(C) of the CFAA should not be read so as to put data researchers at risk for criminal or civil liability for conducting research that involves collecting information that is publicly available on the Internet. *See Sandvig v. Barr*, 2020 U.S. Dist. LEXIS 53631, *24-

5. As used in this brief, the term "scraping" means accessing and collecting data from a webpage using automated means.

6. Indeed, this is how search engines such as Google, Yahoo!, and others function.

43 (D.D.C. March 27, 2020), *appeal filed*, No. 20-5153 (D.C. Cir. May 28, 2020) (researchers accessing publicly accessible data in a manner that violates a website's terms of service do not violate the criminal provisions of the CFAA). A company should not be allowed to use the penalties of the CFAA to prohibit the collection of the information that it posts when that collection is done for *any* purpose, including, for example, determining whether that company has a financial conflict of interest adversely affecting the reliability or objectivity of its data or operations. Companies that allow prospective purchasers of its goods or services to browse its websites must not use the proscriptions of this Section of the CFAA to prohibit scientists, lawyers, or other professionals to do the same for research purposes. Similarly, such companies should not be able to use the CFAA to impede and discourage such research by prohibiting any particular *means* of collecting such information, such as scraping—whether the prohibition is posted in English on the website or posted in code in a "robots.txt" file.[7]

This does not mean that the misuse of the Internet, a website, or a website's data is not actionable, as other statutes are available under state and federal law, both criminal and civil, to prohibit specific instances of misuse.

For example, excessive or inappropriate use of automated search mechanisms may be prohibited by Section 1030(a)(5)(A) of the CFAA, which provides that whoever

7. A convention observed by some indexing services is to look for a file named "robots.txt" on a web site and use its contents as advice on what to index or avoid.

> knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer [commits a federal offense and shall be punished as further provided by Section 1030(c) of the CFAA].

The CFAA provides for a civil remedy for a victim of this offense, found in Section 1030(g). It also allows for injunctive relief.

The theft of data may be the subject of yet other laws:

(1) social security numbers, credit card numbers, and other bank access information are addressed by 18 U.S.C. § 1029 (unauthorized access devices);

(2) confidential business information, including trade secrets, is addressed by the Economic Espionage Act, 18 U.S.C. § 1831 *et seq.*, particularly by Section 1832;

(3) circumvention of an access control device protecting the data, such as a password, or a mandatory question-and-answer page interposed between the viewer and the data, or a paywall; or otherwise hacking into a computer system, including utilizing a software vulnerability or a direct attack on the hardware, is conduct that may be covered by such laws as the wire fraud statute, 18 U.S.C. § 1343; the anticircumvention provisions of the Digital Millennium Copyright Act, 17 U.S.C. § 1201; and the Stored Communications Act, 18 U.S.C. § 2701 *et seq.*;

(4) subsequent dissemination of copyrighted material accessed may be prohibited by copyright law, including

the criminal provisions of the No Electronic Theft Act, 17 U.S.C. § 506(a)(B) & (C); and

(5) taking of government information may be addressed by another provision of the CFAA, 18 U.S.C. § 1030(a)(2)(B), or by 18 U.S. Code § 641 (*see United States v. Morrison*, 844 F.2d 1057 (4th Cir. 1988) (theft and sale to the press of classified government information)).

Another example is the violation of the terms of service for a website. Such a violation may result in a claim for breach of contract and the termination of service to the user who violated the terms of service. There is no reason for the criminal and the civil remedies in the CFAA to be implicated, and no reason for these cases to be litigated in federal courts as opposed to state court venues.

Noteworthy is that equating a violation of the CFAA with a violation of an internet service provider's terms of service, or a violation of an employment agreement concerning the use of a company's computer system, or disregarding the posting of a limitation for the use of a website, will result in the following anomalous judicial situation: private and commercial entities will be empowered to draft criminal laws by means of the language they use in these agreements—enforceable through a bootstrapping process under the CFAA. Under our Constitution, it is up to *Congress* to draft criminal laws—*not* private entities.

D. Automated Scraping Is an Invaluable Tool for Information Technology Professionals

The USTPC urges the Court to recognize fully the need for a narrow interpretation of Section 1030(a)(2)

(C). For this purpose, we include the following examples of scholarly research that have been conducted by data scientists using automated scraping that have had a positive impact within the disciplines of computer science and related fields of science and technology:

1. Emilio Ferrara, Pasquale De Meo, et al., *Web Data Extraction, Applications and Techniques: A Survey,* 70 Knowledge Based Systems 301-23 (Nov. 2014), https://doi.org/10.1016/j.knosys.2014.07.007: Data mining or data extraction from website content using scraping or web crawling techniques is a key tool enabling the performance of analysis in business intelligence systems and can be used to gather data disseminated by social platform users for analysis of human behavior on a large scale.

2. Ensheng Dong, Hongru Du, et al., *An interactive web-based dashboard to track COVID-19 in real time,* The Lancet Infectious Diseases Vol 20 (May 2020), https://doi.org/10.1016/S1473-3099(20)30120-1: Development of an online interactive dashboard that aggregates local media and government reports, and uses twitter feeds and online news services to visualize and track reported COVID-19 cases in real time, including the location and number of confirmed cases, deaths and recoveries for all countries.

3. Nicolas Christin, *Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace,* Proceedings of the International World Wide Web Conference, WWW '13, at 213-224. (Rio de Janeiro, Brazil

May 2013), https://www.andrew.cmu.edu/user/nicolasc/publications/TR-CMU-CyLab-12-018.pdf: Study conducted an economic analysis of dark web markets by daily web crawls, collecting and analyzing data from hidden international marketplaces using Bitcoin exchange currency, concluding that the Silk Road service was used as a market for controlled substances and narcotics.

4. Kyle Soska and Nicolas Christin, *Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem*, Proceedings of the 24th USENIX Security Symposium (USENIX Security 2015) at 33-48. (Washington, DC August 2015), https://dl.acm.org/doi/10.5555/2831143.2831146: Researchers conducted a two-year analysis of the anonymous online marketplace ecosystem, the goods sold, the marketplace economics, and the effectiveness of law enforcement, leading to policy developments such as the European Monitoring Centre for Drugs and Drug Addiction (EMCDDA) and EUROPOL.

5. Arunesh Mathur, Gunes Acar, et al., *Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites,* Proceedings of the ACM on Human-Computer Interaction (Nov. 2019), https://doi.org/10.1145/3359183: Researchers used automated data mining techniques, analyzing 11,000 websites to identify so-called "dark patterns" on shopping websites that seek to coerce, steer or deceive users into making unintended or harmful decisions. Deceptive practices were identified on 183 sites, and

recommendations were made for researchers and regulators to address these patterns.

6. Timothy Libert, *An Automated Approach to Auditing Disclosure of Third-Party Data Collection in Website Privacy Policies*, Proceedings of the World Wide Web Conference, WWW '18 (Lyon, France April 23–27, 2018), https://doi.org/10.1145/3178876.3186087: Conducted large scale audit of disclosure of data collection in website privacy policies, analyzing data flows from one million websites alongside 200,000 privacy policies, finding that, although third party data collection is widespread, fewer than 15% of data flows are disclosed, indicating that most implementations of "notice and choice" provisions are ineffective.

7. Daniel Trielli and Nicholas Diakopoulos, *Search as News Curator: The Role of Google in Shaping Attention to News Information*, CHI 2019 (Glasgow, Scotland, UK May 4-9, 2019), http://www.nickdiakopoulos.com/wp-content/uploads/2019/04/Search-as-News-Curator.pdf: Using an algorithm audit of Google Top Stories box to demonstrate source concentration and ideological skew of news, and subsequent shifts in traffic and addition for publishers of news.

8. Daniel Trielli & Nicholas Diakopoulos, *Partisan search behavior and Google results in the 2018 U.S. midterm elections,* Information, Communication & Society (2020), https://www.tandfonline.com/doi/full/10.1080/1369118X.2020.1764605: Study collected search terms

from people with differing ideological positions concerning Senate candidates in the 2018 midterm election and used those search terms to scrape web results. The study found that Google results exhibit a "mainstreaming effect" that partially neutralizes differentiation of search by providing a set of common results, even to dissimilar searches.

9. Aniko Hannak, Piotr Sapiezynski, et al., *Measuring Personalization of Web Search*, World Wide Web Conference 2013, WWW '13, at 527–538 (2013), https://doi.org/10.1145/2488388.2488435: Demonstrating methodology to measure personalization in Web search results that may prevent certain users from accessing information that the search engine's algorithm decides is irrelevant.

10. Christian Sandvig, Kevin Hamilton, et al., *Auditing Algorithms: Research Methods for Detecting Discrimination on Internet Platforms*, Paper presented to the International Communication Association (Seattle, WA, USA May 22, 2014), http://www-personal.umich.edu/~csandvig/research/Auditing%20Algorithms%20--%20Sandvig%20--%20ICA%202014%20Data%20and%20Discrimination%20Preconference.pdf: Supporting the use of data mining tools to develop methods to audit algorithms used in large Internet platforms to determine the existence of bias that may lead to negative outcomes based on race, gender or class.

11. Le Chen, Ruijun Ma, et al., *Investigating the Impact of Gender on Rank in Resume Search Engines,* Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, 1–14 (2018), https://doi.org/10.1145/3173574.3174225; Investigating gender-based inequalities in resume search engines by collecting search results on major online job boards for 855,000 job candidates, to provide a statistical indication of discrimination or unfairness.

12. Anikó Hannák, Claudia Wagner, et al., *Bias in Online Freelance Marketplaces: Evidence from TaskRabbit and Fiverr*, CSCW 2017, (Portland, OR, USA February 25–March 1, 2017), https://dl.acm.org/doi/abs/10.1145/2998181.2998327: Collecting and analyzing 13,500 worker profiles and information concerning the workers' gender, race, customer reviews, ratings and positions in search rankings examining whether two prominent online freelance marketplaces are affected by racial and gender bias.

13. Luz Rello and Ricardo Baeza-Yates, *Lexical Quality as a Measure for Textual Web Accessibility*, ICCHP 2012, Part I, Springer LNCS 7382 at 404-08 (Linz, Austria July 2012): Using scraping of text on websites to evaluate accessibility of the sites for dyslexic users and presenting a model that provides recommendations for better accessibility in web content.

14. Venkatadri, Giridhari, Elana Lucheruni, et al., *Investigating sources of PII used in Facebook's targeted advertising.* PoPETs at 227-244 (2018), https://mislove.org/publications/PII-PETS.pdf: Investigating the sources of personally identifiable information (PII) used for targeted advertising in Facebook, finding that user phone numbers and email addresses are used by Facebook to allow its advertisers to target users.

15. Asplund, J., Eslami, M., Sundaram, et al., *Auditing Race and Gender Discrimination in Online Housing Markets*, Proceedings of the International AAAI Conference on Web and Social Media, Vol. 14 at 24-35 (2020), https://www.aaai.org/ojs/index.php/ICWSM/article/view/7276: Demonstrating a technique for building online profiles to audit Fair Housing Act compliance. Results of investigation demonstrate that indirect discrimination occurs in the number and type of housing ads served based on the user's race, as well as in property recommendations based on the user's gender.

16 Jayant Madhavan, David Ko, et al., *Google's Deep-Web Crawl*, PVLDB 2008 (Auckland, New Zealand August 23-28, 2008): Describing a novel system for surfacing Deep-Web content in coverage of search engines, including an algorithm to navigate the search space and identify URLs suitable for inclusion in a web search index.

17. Ansley Post, Vijit Shah, et al., *Bazaar: Strengthening user reputations in online*

marketplaces, PROCEEDINGS OF THE SYMPOSIUM ON NETWORKED SYSTEM DESIGN AND IMPLEMENTATION (NSDI) (Boston, MA, USA, Mar 2011), http://www.usenix.org/events/nsdi11/tech/full_papers/Post.pdf: Proposing a novel system that calculates user reputations using data from prior successful transactions to limit reputation manipulation.

18. Arash Molavi Kakhki, Chloe Kliman-Silver, et al., *Iolaus: Securing Online Content Rating Systems*, PROCEEDINGS OF THE INTERNATIONAL WORLD WIDE WEB CONFERENCE, WWW '13 (Rio de Janeiro, Brazil May 2013), https://mislove.org/publications/Iolaus-WWW.pdf: Using, *inter alia*, content rating data to demonstrate the effectiveness of a novel system to protect against multiple-identity and rating-buying attacks.

19. Le Chen, Alan Mislove, et al., *An Empirical Analysis of Algorithmic Pricing on Amazon Marketplace,* PROCEEDINGS OF THE INTERNATIONAL WORLD WIDE WEB CONFERENCE, WWW '16 (Montréal, Canada April 2016), https://dl.acm.org/doi/10.1145/2872427.2883089: Using data about best-seller products on Amazon Marketplace to determine the algorithmic pricing strategies used by sellers, and to characterize the effects of these strategies on marketplace dynamics.

20. Shan Jiang, Le Chen, et al., *On Ridesharing Competition and Accessibility: Evidence from Uber, Lyft, and Taxi,* PROCEEDINGS OF THE INTERNATIONAL WORLD WIDE WEB CONFERENCE, WWW '18 (Lyon, France April 2018), https://personalization.ccs.neu.edu/static/pdf/jiang-

www18.pdf: Comparing Uber, Lyft and taxi data to develop statistical techniques to examine the relationship of transportation infrastructure and socioeconomic influences on Vehicle for Hire market features.

CONCLUSION

A Bright Line Test

Where information is made publicly available on the Internet, Section 1030(a)(2)(C) of the CFAA cannot be interpreted as prohibiting any *means* of accessing that information, and cannot be construed as prohibiting any *motive* for accessing that information, by terms of service, employment agreements, company policies, or the postings of any limitation of use.

Publicly disclosed information is publicly available. This is a bright line in the sand.[8]

Dated: July 8, 2020

Respectfully submitted,

Arnon D. Siegel, Esq.
655 Avenue of the Americas
New York, New York 10010

Andrew Grosso
Counsel of Record
Mark D. Rasch
Ronald J. Jarvis
Andrew Grosso & Associates
1101 Thirtieth Street NW,
Suite 500
Washington, D.C. 20007
(202) 298-6500
agrosso@acm.org

Counsel for Amicus Curiae

8. And we note that sand is primarily silicon.

APPENDIX

APPENDIX — MEMBERS ON THE BRIEF

U.S. Technology Policy Committee[1]
Association for Computing Machinery
1701 Pennsylvania Avenue, NW, Suite 200
Washington, DC 20006
(202) 580-6555

James Hendler, Ph.D. (Computer Science)
Chair, ACM U.S. Technology Policy Committee
Fellow of the ACM, AAAS and National Academy of Public Administration
Member, National Security Directorate PNNL Directors Advisory Committee
Member, National Academies Board on Research Data and Information
Member, Homeland Security Science and Technology Advisory Committee
Open Data Advisor, New York State
US Air Force Exceptional Civilian Service Medal
Director, Rensselaer Institute for Data Exploration and Applications
Rensselaer Polytechnic Institute

Alec Yasinsac, Ph.D. (Computer Science)
Vice Chair, ACM U.S. Technology Policy Committee
Professor and Dean, School of Computing
University of South Alabama

1. Beyond the USTPC, the views of the persons listed in this Appendix do not necessarily represent the views of the organizations with which they are associated.

Appendix

Mubasher Ahmed, MBA (Finance), M.S. (Computer Science), COBIT, TOGAF, ITIL, CPHIMS, PAHM
Independent Consultant

Ricardo Baeza-Yates, Ph.D. (Computer Science)
Fellow of the ACM and IEEE
Director of Data Science
Northeastern University, Silicon Valley

Vinton Cerf, Ph.D. (Computer Science)
Internet Pioneer
Past President, Association for Computing Machinery
Fellow of the ACM, IEEE, and Association of Women in Science
U.S. Presidential Medal of Freedom
National Medal of Technology
ACM A.M. Turing Award
Internet Hall of Fame Pioneer
National Inventors Hall of Fame
IEEE Alexander Graham Bell Medal
Marconi Prize
Prince of Asturias Award
Japan Prize
Queen Elizabeth Prize for Engineering
Benjamin Franklin Medal
Founder and Former Chair, Internet Corporation for Assigned Names and Numbers

Nicolas Christin, Ph.D. (Computer Science)
Associate Professor of Computer Science and Engineering & Public Policy
Carnegie Mellon University

Appendix

Lorrie Faith Cranor, D.Sc. (Engineering and Policy), CIPT
Fellow of the ACM and IEEE
Director and Bosch Distinguished Professor in Security and Privacy Technologies
CyLab Security and Privacy Institute
FORE Systems Professor of Computer Science and Engineering & Public Policy
Carnegie Mellon University

William E. J. Doane, Ph.D. (Informatics)
Research Staff Member
IDA Science and Technology Policy Institute

Andrew Grosso, J.D., M.S. (Physics), M.S. (Computer Science)
Chair, U.S. Technology Policy Committee Law Subcommittee
Andrew Grosso & Associates

Mark P. Hahn, CISSP, CSM
Director, Cloud Strategies and DevOps
Ciber Global LLC

Rebecca Herold, M.A. (Computer Science and Education), FIP, CISSP, CIPP/US, CIPT, CIPM, CISM, CISA, FLMI
Fellow of the Ponemon Institute
Top 100 Women Fighting Cybercrime
CEO and Founder
The Privacy Professor Consultancy

Appendix

Harry Hochheiser, Ph.D. (Computer Science)
Chair, ACM U.S. Technology Policy Committee Accessibility Subcommittee
Associate Professor of Biomedical Informatics
University of Pittsburgh
Director, Biomedical Informatics Training Program
University of Pittsburgh School of Medicine

Lance J. Hoffman, Ph.D. (Computer Science)
Fellow of the ACM
Member, Cybersecurity Hall of Fame
Distinguished Research Professor
The George Washington University

Paul E. Hyland, M.A. (Science, Technology and Public Policy), MCP
Senior Member of the ACM
Chair, ACM U.S. Technology Policy Committee IP Subcommittee
Senior Director, UX Development & Operations
Higher Digital
Adjunct Assistant Professor, Digital Media and Web Technology
University of Maryland Global Campus

Douglas W. Jones, Ph.D. (Computer Science)
Associate Professor of Computer Science
University of Iowa

Appendix

Meg Leta Jones, J.D., Ph.D. (Technology, Media, & Society)
Associate Professor
Communication, Culture & Technology
Georgetown University

Cem Kaner, J.D., Ph.D. (Psychology)
Member of the American Law Institute
Recipient, ACM SIGCAS Making a Difference Award
Professor Emeritus of Software Engineering
Florida Institute of Technology

Lorraine Kisselburgh, Ph.D. (Media, Technology, and Society)
Chair, ACM Technology Policy Council, Association for Computing Machinery
Lecturer and Visiting Fellow (*retired Faculty*)
Purdue University

Aaron Massey, Ph.D. (Computer Science)
Assistant Professor of Software Engineering
University of Maryland, Baltimore County

Jeanna Neefe Matthews, Ph.D. (Computer Science)
Member, ACM Council
Member, ACM Technology Policy Council
Co-Chair, ACM U.S. Technology Policy Committee
AI & Algorithms Subcommittee
Professor of Computer Science
Clarkson University

Appendix

John M. Murray, Ph.D. (Engineering Science)
General Manager
Calidris Partners
Research Director
Linqto Inc.

Peter G. Neumann, Ph.D. (Applied Mathematics) and Dr. rerum naturalium (Math & Physics), CISSP (honorary)
Fellow of the ACM, IEEE, and AAAS
Member, U.S. General Accounting Office information Technology Executive Council
Member, National Science Foundation Computer Information Science and Engineering Advisory Board
Chief Scientist, Computer Science Laboratory
SRI International

Mark Rasch, J.D., Ph.D. (Public Policy)
Of Counsel
Andrew Grosso & Associates
Professorial Lecturer of Law
George Washington University School of Law

Arnon Rosenthal, Ph.D. (Computer Science)
The MITRE Corporation

Appendix

Pamela Samuelson, J.D.
Fellow of the ACM
Contributing Editor, Communications of the ACM
Fellow of the John D. & Catherine T. MacArthur Foundation
Director, Berkeley Center for Law & Technology
Richard M. Sherman Distinguished Professor of Law and Information
University of California, Berkeley

Ben Shneiderman, Ph.D. (Computer Science)
Fellow of the ACM, AAAS and National Academy of Inventors
Member, National Academy of Engineering
ACM SIGCHI Lifetime Achievement Award
IEEE Visualization Career Award
Founding Director, Human Computer Interaction Lab
Distinguished University Professor of Computer Science
University of Maryland Institute for Advanced Computer Studies
University of Maryland, College Park

Barbara Simons, Ph.D. (Computer Science)
Past President, Association for Computing Machinery
Founding Chair, ACM U.S. Technology Policy Council
Co-Chair, ACM U.S. Technology Policy Committee Voting Subcommittee
Fellow of the ACM and AAAS
ACM Policy Award
IBM Research (*retired*)

Appendix

Oliver R. Smoot, J.D. (*retired*)
Past President, International Organization for Standardization
Past Chairman of the Board, American National Standards Institute
Past President, Computer Law Association (*now ITechLaw Association*)
Past Chair, Science and Technology Law Section of the American Bar Association
George S. Wham Medal, American National Standards Institute
Leo B. Moore Medal, Standards Engineering Society

Eugene H. Spafford, Ph.D., D.Sc. (Computer Science)
Fellow of the AAAS, ACM, IEEE, AAA&S, $(ISC)^2$, and Distinguished Fellow of the ISSA
Member, Cyber Security Hall of Fame
Professor and Executive Director Emeritus, Center for Education and Research in Information Assurance and Security
Purdue University

Patrick Traynor, Ph.D. (Computer Science and Engineering)
Research Fellow of the Alfred P. Sloan Foundation
John and Mary Lou Dasburg Preeminence Chair in Engineering
Professor of Computer Science and Engineering
Herbert Wertheim College of Engineering
University of Florida

Appendix

Kashyap R. Tumkur, M.S. (Computer Science)
ACM Future of Computing Academy
Senior Software Engineer