Bloomberg BNA

Electronic Commerce & Law Report™

BIG DATA

A new lawsuit filed by the American Civil Liberties Union presents a novel theory that, if adopted, could invalidate sections of the federal computer fraud statute as some courts have interpreted it. Attorneys from Wiley Rein LLP discuss the novel theory, the ACLU's interest in the case and its potential to impact federal law governing online commerce.

ACLU Suit Attacks Computer Fraud and Abuse Act to Investigate Website Discrimination Using Controversial Online Tactics




By Megan L. Brown, Stephen J. Obermeier, Matthew J. Gardner and Stephen J. Kenny

The White House, Federal Trade Commission and others have aired concerns about discrimination online, sometimes referred to as ''digital redlining'' (21 ECLR 924, 6/8/16). Several Executive Branch reports have identified potential effects of technology and ''big data'' that could harm protected classes. Citing those reports, the American Civil Liberties Union has sued on behalf of several professors, seeking to invalidate part of the Computer Fraud and Abuse Act (''CFAA'').

Megan L. Brown,Stephen J. Obermeier, Matthew J. Gardner and Stephen J. Kenny are attorneys at Wiley Rein LLP in Washington. Ms. Brown is a partner in the Cybersecurity, Appellate, and TMT practices. Mr. Obermeier is a partner in the Appellate, Litigation, and Telecom, Media & Technology practices. Mr. Gardner is of counsel in the White Collar Defense & Government Investigations and Cybersecurity practices. Mr. Kenny is an associate in the Election Law & Government Ethics and Litigation practices.

The ACLU wants to help researchers and others test websites and algorithms for discriminatory impact by ''scraping'' data from sites and using ''bots'' impersonating legitimate users. The ACLU asserts that part of the CFAA impedes that testing, and asks a judge to invalidate the provision.

The novel suit faces an uphill climb but sheds light on theories companies may face in the future. It demonstrates the increased interest in investigating digital redlining, and promotes the use of controversial techniques which could have unintended consequences for online security.

 ISSN 1098-5190

The ACLU Seeks to Strike Part of a Key Federal Law

The CFAA imposes criminal and civil penalties on those who intrude or unlawfully access computers and networks. It has broad application and has been used to sanction individuals, often disgruntled employees or competitors, who break into networks or exceed authorizations to access digital information. It has been an important tool in protecting and securing computer and communications systems, and many have called for more aggressive use of it in prosecuting online crimes.

The ACLU asks the court to invalidate 18 U.S.C. § 1030(a)(2)(C), which creates liability when an individual, in accessing a protected computer, does so in a manner that ''exceeds authorized access.'' The ACLU says that ''[c]ourts and federal prosecutors have interpreted the prohibition on 'exceed[ing] authorized access' to make it a crime to visit a website in a manner that violates the terms of service or terms of use . . . established by that website. The Challenged Provision thereby delegates power to companies that operate online to define the scope of criminal law through their own terms of service.''

The ACLU makes novel constitutional claims on behalf of academics who say they fear that the CFAA criminalizes their desired research. They assert violations of the First Amendment rights of freedom of speech and the press, claiming the CFAA ''prevents speech and expressive activity necessary to inform and influence the decisions of the public and the government in online discrimination'' including regulators and enforcement offices of several agencies.

The ACLU also claims the CFAA violates their Fifth Amendment due process rights, because it is void for vagueness and an unlawful delegation of lawmaking power to private entities; namely the companies whose terms and conditions govern access and restrict use of their websites.

The Suit Provides Roadmap of Future Discrimination Theories

The lawsuit seems likely to face challenges on ripeness and standing, as well as on the merits. Regardless of the merit of the lawsuit, it marks an escalation and provides a detailed explanation of the theories and tactics likely to be used against online companies by plaintiffs seeking to substantiate theories of disparate impact. The ACLU expresses fear about potential aspects of online commerce and activity.

A few examples of its areas of concern are that:

■ ''[P]rofiles can follow individuals online, enabling websites and advertisers to display content targeted at, for example, African-American visitors or women.''

■ ''Tracking technologies, which allow websites and advertisers to compile records of individuals' browsing histories, also allow for targeting.''

■ ''Algorithms seek to discern correlations in existing data sets in order to predict which factors correlate with desired outcomes. But the use of such algorithms could result in disparate outcomes for members of protected classes. For example, if an existing data set concerning past hiring decisions reflects past discrimination, a hiring algorithm may avoid Latinos because Latinos were historically less likely to be hired.''

The ACLU is concerned about ''real estate, finance, and employment transactions'' migrating online, and wants to test ''the potential for harmful online discrimination by internet platforms'' and of varied ''advertising networks and exchanges'' that operate online.

The ACLU Promotes Techniques—Bots and Scraping—with Unintended Consequences

The tactics featured by the ACLU are controversial because they can raise security and other concerns. For example, Plaintiffs propose to ''develop an automated program or agent browsing the Web, referred to as a 'bot.' Each bot represents an individual person and is designed to interact with a website as a user might. It can visit websites, click links, fill out and submit forms, collect and store information from a web page, and do other things automatically, based on scripts written by Plaintiffs. . . . The bot will be instructed to behave as a number of different users; each of these profiles is a 'sock puppet.' '' They also would like to ''scrape'' information from websites they visit.

Bots and scraping are complex and have trade-offs; industry has developed tools to manage their use. Indeed, Plaintiffs acknowledge that ''[t]he use of bots is prohibited by many websites that the bot would visit in the course of building the racially-identifiable sock puppets. Scraping is prohibited by the terms of service of virtually all real estate websites.''

For good reason. The use of bots to create fake registrations threatens to distort companies' data sets and business operations. As one commenter explains, databases that receive spam registration by bots can become ''infused with fake data. This skews their data thereby decreasing the credibility of the database. Without accurate data available, these websites have difficulty attracting others to advertise on their site and won't know for sure who their typical user is.'' Ironically, this would exacerbate the concern about imperfect data sets that seems to concern the Plaintiffs.

As for scraping, accessing and pulling information off websites has been subject to legal dispute for decades, as companies from eBay to Facebook protect their sites and content from competitors and others. There are serious and legitimate concerns about scraping, which has federal and state law implications. The ACLU's request for an exception from the potential reach of the CFAA for some uses of these techniques could have serious and unpredictable practical consequences.

Those urging a rollback of the CFAA note that, of the many amendments since its enactment, none grapple with independent security researchers' and hackers' roles in addressing security threats and vulnerabilities. This is not surprising because in an area of technology, law and policy this complex, it is hard to envision a workable approach that treats as dispositive a hacker's subjective intent or status as a ''researcher.'' In the world of online security the difference between ''white hats'' and ''black hats'' is not always clear.

In bringing this suit, the ACLU is firing a shot across the bow of the digital economy. Regardless of its ultimate merit, the novel claims preview a future of increased scrutiny for online operators, as skeptical third

   ISSN 1098-5190

parties and government regulators seek transparency into big data, algorithms, and targeted advertising to ferret out so-called digital redlining. The lengths to which the ACLU goes in this suit to promote the investigation of digital redlining offers another signal that the interest in this is substantial and can only be expected to increase.