SCOTUS Guts Purpose-Based Policy Claims Under the Computer Fraud and Abuse Act

6.10.2021

In *Van Buren v. United States*, a recently released 6-3 decision, authored by our newest Supreme Court Justice, Amy Coney Barrett, the Supreme Court resolved a long-brewing circuit split in the interpretation of the Computer Fraud and Abuse Act (CFAA). The Court addressed the issue of whether a person who is authorized to access information on a computer for certain purposes violates the CFAA if the person accesses that information for an improper purpose. The Court held that a person does not "exceed authorized access" in violation of the CFAA by misusing access to obtain information that is otherwise available to that person.

The case involved a police sergeant caught in an FBI sting operation using a law enforcement database—for which he was authorized to access—to obtain information for an FBI informant's personal use in exchange for money. The sergeant's conduct violated the police department's purpose-based policy against obtaining database information for non-law enforcement purposes. The sergeant was subsequently convicted of violating the CFAA and later appealed the conviction.

Passed in 1986, the CFAA prohibits a person from "intentionally access[ing] a computer without authorization or ***exceed[ing] authorized access***." The phrase "exceeds authorized access" is defined as meaning "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." While the CFAA is a criminal statute, because it also provides for a civil remedy, businesses have successfully raised it against employees who misused their computer authorization to misappropriate trade secrets and confidential information. As such, *Van Buren* has vast implications for these civil litigants.

Related Services

Non-Compete & Trade Secret

Trade Secret & Non-Compete Specialty Team

Prior to *Van Buren*, the circuit courts were divided as to whether a person exceeded authorized access by obtaining information from a computer for an improper purpose, including misappropriating it for personal purposes unrelated to the access granted. For example, an employer would argue that an engineer who downloaded the proprietary design for a self-driving vehicle she had been working on to take to her new employer "exceeded her access" even though she had access to the design to do her job. But whether this violated the CFAA depended on the circuit where the claim was litigated. Siding with the circuits that more narrowly interpreted the CFAA, the Court found that the CFAA, does not "cover those who … have improper motives for obtaining information that is otherwise available to them." In our example, the engineer, therefore, is not liable for violating the CFAA.

While clearly foreclosing claims relating to purpose-based access restriction once available in many circuits, the Court failed to address whether the CFAA prohibits use-based access restrictions on categories of information that are not related to the access granted to the employee. Getting back to our earlier example, let's assume company policy prohibits the engineer from accessing information unrelated to her design assignment, but the company neither encrypts nor restricts access to data unrelated to the engineer's scope of work. With her unrestricted network access in hand, if our engineer working on autonomous vehicle design instead decides to access proprietary research data related to vehicle emissions that was openly available to her in the company network, would her conduct violate the CFAA? There is no clear answer.

After *Van Buren*, employees have more certainty that they are not in danger of a committing a federal crime when they make an amazon purchase or check sports scores on their work computer. But employers are left with fewer remedies and more questions. Employers may consider reworking their policies. Butzel Long's Non-Compete and Trade Secret attorneys are at the ready to assist and advise should your business need assistance following *Van Buren*.

A special thanks to Butzel Long Summer Associate Christine Santourian for her help in putting this client alert together. Ms. Santourian is a rising 2L at the University of Detroit-Mercy School of Law and received her undergraduate degree from the University of Michigan, Ann Arbor in 2014.

Sarah Nirenberg
248.258.2912
nirenberg@butzel.com

Bernie Fuhs
313.225.7044
fuhs@butzel.com

Claudia Rast
734.213.3431
rast@butzel.com