The New York Times

Business/Financial Desk; SECTB

Trial Is Test Of U.S. Law On Hacking

By Kate Conger
1,308 words
9 June 2022
The New York Times
NYTF
Late Edition - Final
1
English

A woman is accused of downloading data of more than 100 million Capital One customers. Her lawyers argue a conviction would criminalize legitimate research practices.

Nearly three years after the disclosure of one of the largest data breaches in the United States, the former Amazon employee accused of stealing customers' personal information from Capital One is standing trial in a case that will test the power of American anti-hacking law.

Paige Thompson worked as a software engineer in Seattle and ran an online community for other programmers. In 2019, she downloaded personal information belonging to more than 100 million Capital One customers, the Justice Department said.

The data came from applications for credit cards, and included 140,000 Social Security numbers and 80,000 bank account numbers. She faces 10 counts of computer fraud, wire fraud and identity theft in a federal trial that began on Tuesday in Seattle.

The methods Ms. Thompson used to discover the information, and what she planned to do with it, will be closely scrutinized in the case. Ms. Thompson, 36, is accused of violating an anti-hacking law known as the Computer Fraud and Abuse Act, which forbids access to a computer without authorization. Ms. Thompson has pleaded not guilty, and her lawyers say her actions -- scanning for online vulnerabilities and exploring what they exposed -- were those of a ''novice white-hat hacker.''

Critics of the computer fraud law have argued that it is too broad and allows for prosecutions against people who discover vulnerabilities in online systems or break digital agreements in benign ways, like using a pseudonym on a social media site that requires users to go by their real names.

In recent years, courts have begun to agree. The Supreme Court narrowed the scope of the law last year, ruling that it could not be used to prosecute people who had legitimate access to data but exploited their access improperly. And in April, a federal appeals court ruled that automated data collection from websites, known as web scraping, did not violate the law. Last month, the Justice Department told prosecutors that they should no longer use the law to pursue hackers who engaged in ''good-faith security research.''

Ms. Thompson's trial will raise questions about how far security researchers can go in their pursuit of **cybersecurity** flaws before their actions break the law. Prosecutors said Ms. Thompson had planned to use the information she gathered for identity theft, and had taken advantage of her access to corporate servers in a scheme to mine cryptocurrency. But her lawyers have argued that Ms. Thompson's discovery of flaws in Capital One's data storage system reflected the same practices used by legitimate security researchers and should not be considered criminal activity.

''They are interpreting a statute so broadly that it captures conduct that is innocent and as a society we should be supporting, which is security researchers going out on the internet and trying to make it safer,'' said Brian Klein, a lawyer for Ms. Thompson. The law ''doesn't give a lot of visibility to people on what could get you in trouble and what couldn't get you in trouble,'' Mr. Klein added.

The Justice Department has argued that Ms. Thompson had no interest in helping Capital One plug the holes in its security and that she cannot be considered a ''white hat'' hacker. Instead, she chatted with friends online about how she might be able to profit from the breach, according to legal filings.

''Even if her actions could be broadly characterized as 'research,' she did not act in good faith,'' Nicholas W. Brown, the U.S. attorney for the Western District of Washington, wrote in a legal filing. ''She was motivated both to make money and to gain notoriety in the hacking community and beyond.''

Some security researchers said Ms. Thompson had ventured too far into Capital One's systems to be considered a white-hat hacker.

"Legitimate people will push a door open if it looks ajar," said Chester Wisniewski, a principal research scientist at Sophos, a **cybersecurity** firm.

It is not uncommon for security researchers to test vulnerabilities they discover, making sure that they result in flaws that expose data, before reporting the problems to companies so they can be fixed. But downloading thousands of files and setting up a cryptocurrency mining operation were "intentionally malicious actions that do not happen in the course of testing security," Mr. Wisniewski said.

Ms. Thompson grew up in Arkansas, where she struggled to fit in but excelled with computers, according to court records. She dropped out of high school and made plans to move to Seattle, where she would eventually join a thriving community of technologists and begin a gender transition.

In 2005, before she turned 20, Ms. Thompson was already working in a series of software development jobs. In 2015, she secured a job at Amazon Web Services, the **cloud computing** wing of the online retail giant, and worked there for a little over a year. But Ms. Thompson occasionally struggled with her mental health and at times felt alienated from her peers in the tech industry, who she worried did not accept her transition, she wrote on social media and a personal blog.

Just as Amazon stores millions of physical goods in a dizzying array of warehouses, Amazon Web Services hosts vast amounts of data for other companies that rent space on its servers. Among its customers was Capital One.

In early 2019, several years after she stopped working for Amazon Web Services, Ms. Thompson searched for its customers who had not properly set up firewalls to protect their data. "Thompson scanned tens of millions of AWS customers looking for vulnerabilities," Mr. Brown wrote in a legal filing. By March, she had discovered a vulnerability that allowed her to download data from Capital One, the prosecutor added.

In June 2019, Ms. Thompson sent online messages to a woman and disclosed what she had found, legal filings said. Ms. Thompson added she had considered sharing the data with a scammer, and said she would publicly reveal her involvement in the breach.

"I've basically strapped myself with a bomb vest," Ms. Thompson said in copies of the online chat that were included in court records, referring to her plan to publicly release the data and expose herself.

The woman suggested that Ms. Thompson turn herself in to the authorities, prosecutors said. A month later, the woman contacted Capital One and told the bank about the breach. Capital One informed law enforcement officials, and Ms. Thompson was arrested in late July 2019. If convicted, she could face more than 30 years in prison.

"The snapshots submitted by the government are an incomplete and inaccurate portrayal of a life more fairly described as one of survival and resilience," Mohammad Ali Hamoudi, a lawyer representing Ms. Thompson, and other members of her legal team wrote in a filing. Ms. Thompson had sought mental health treatment, they added, demonstrating her resolve to confront her problems.

In 2020, Capital One agreed to pay $80 million to settle claims from federal bank regulators that it lacked the security protocols needed to protect customers' data. The settlement also required the bank to work quickly to improve its security. In December, Capital One agreed to pay $190 million to people whose data had been exposed in the breach, settling a class-action lawsuit.

Paige Thompson is accused of downloading the personal data of more than 100 million Capital One customers. Her federal trial began on Tuesday. (PHOTOGRAPH BY EMON HASSAN FOR THE NEW YORK TIMES); Lawyers for Ms. Thompson argue that she was a "white-hat hacker" acting in good faith to research flaws in security. (B4)

Document NYTF000020220609ei690003o

Search Summary

Text	(technology OR "AI" OR fintech OR "digital banking" OR "cloud computing" OR blockchain OR cybersecurity OR "machine learning" OR "data analytics" OR "big data" OR "predictive analytics" OR "cloud migration" OR "edge computing" OR "5G banking" OR "API banking" OR "open banking" OR "data governance" OR "data monetization" OR "digital transformation" OR "quantum computing" OR "AI-driven banking" OR "AI in compliance" OR "AI-powered fraud detection" OR "AI in customer service" OR "AI in investment banking" OR "conversational AI" OR "generative AI" OR "robo-advisors"

	OR "natural language processing" OR "algorithmic trading" OR "automated risk assessment" OR "AI regulatory challenges" OR "embedded finance" OR neobanks OR "Banking as a Service" OR "BaaS" OR regtech OR suptech OR "decentralized finance" OR DeFi OR "cryptocurrency adoption" OR "Central Bank Digital Currencies" OR CBDCs OR tokenization OR "real-time payments" OR "Buy Now Pay Later" OR BNPL OR "cyber resilience" OR "Zero Trust security" OR "identity verification" OR "fraud detection" OR "insider threats" OR "AI-driven cybersecurity" OR "financial data breaches" OR "data privacy laws" OR GDPR OR CCPA OR "operational risk management" OR "regulatory compliance technology" OR KYC OR "Know Your Customer" OR AML OR "Anti-Money Laundering" OR "hyper-personalization in banking" OR "customer-centric banking" OR "omnichannel banking" OR "digital wallets" OR "contactless payments" OR "voice banking" OR "biometric authentication" OR "wearable banking" OR "banking UX/UI innovations" OR "financial inclusion technology")
Date	04/01/2022 to 06/30/2022
Source	The New York Times Or The Wall Street Journal Or The Economist Or Forbes
Author	All Authors
Company	Capital One Financial Corporation
Subject	All Subjects
Industry	All Industries
Region	All Regions
Language	English
Results Found	1
Timestamp	7 March 2025 3:33 AM GMT