Cybersecurity and Information Security Newsletter

Issue 20 | July 7, 2022

Table of Contents

- Senate bill aims to implement export controls to protect personal data from unfriendly nations
- Attorneys serve an anonymous defendant using an NFT

Daniel Shin, research scientist with the Commonwealth Cyber Initiative (CCI) Coastal Virginia region, wants to hear from you! Submit any cybersecurity and information security news items or request related topics, via e-mail to dshin01@wm.edu.

This newsletter supports the mission of CCI. To learn more about CCI, including upcoming events, funded research, and news, please visit cyberinitiative.org.

Senate bill aims to implement export controls to protect personal data from unfriendly nations

On June 24, 2022, U.S. Senator Ron Wyden (D-OR) introduced the *Protecting Americans' Data From Foreign Surveillance Act of 2022*, which aims to implement certain export controls to protect individual personal data in the U.S. *S.4495 - A bill to amend the Export Control Reform Act of 2018 to require export controls with respect to certain personal data of United States nationals and individuals in the United States, and for other purposes*, available here. The bill is intended to protect sensitive personal data "from falling into the hands of malign foreign actors," by requiring export licenses when such information is sold or transferred to high-risk foreign countries.

Senator Wyden notes that current export and other regulations allow foreign companies to purchase databases of sensitive personal data of individuals from data brokers, which can lead to foreign government entities seizing that information. *Wyden, Lummis, Whitehouse, Rubio and Hagerty Introduce Bipartisan Legislation to Protect Americans' Private Data from Hostile Foreign Governments*, available here. By implementing new export controls over such data, the bill seeks to protect the privacy rights of individuals in the U.S. Senator Marco Rubio (R-FL), a cosponsor of the bill, comments that the bill also addresses national security threat concerns arising out of unrestricted export of personal data. *Id.*

The bill would amend the *Export Control Reform Act of 2018*, directing the U.S. Department of Commerce to create new export regulations targeting transfers of sensitive personal information of U.S.-based individuals. Specifically, the Secretary of Commerce would be required to identify the categories of personal data that could harm U.S. national security interests if that data were to be exported abroad. Also, the Secretary would identify "high-risk" countries based on:

1. the adequacy and enforcement of data protection, surveillance, and export control laws of the foreign country;
2. the likelihood of the foreign government to compel, coerce, or pay a person to disclose the covered personal data; and
3. whether that government has conducted hostile foreign intelligence operations (including information operations) against the United States. *S.4495, 117th Cong. (2022),* available here.

Export of personal data to low-risk countries would not be restricted, but export to certain other countries would require a license under the bill. Exporting personal data to high-risk countries would be presumptively denied.

Currently, the Senate bill has four cosponsors and has been referred to the Senate Committee on Banking, Housing, and Urban Affairs. *All Actions S.4495 — 117th Congress (2021-2022)*, available here.

Analysis

The collection of sensitive personal data by foreign companies has been a national security concern. For example, on August 6, 2020, former President Trump issued two executive orders affecting the mobile app WeChat and TikTok over concerns that collected personal information from those apps could be used by the Chinese Communist Party (CCP). *Exec.*

Order No. 13942, 85 FR 48637, available here; *Exec. Order No. 13943, 85 FR 48641*, available here. Although recognizing the national interest concerns arising out of hostile nations obtaining personal data of individuals in the U.S., President Biden rescinded executive orders targeting WeChat and TikTok, potentially due to the lack of evidence supporting collusion allegations with the CCP. *Exec. Order No. 14034, 86 FR 31423*, available here ("The Federal Government should evaluate these threats through rigorous, *evidence-based analysis* and should address any unacceptable or undue risks consistent with overall national security, foreign policy, and economic objectives . . . .") (emphasis added).

This Senate bill takes a more comprehensive approach to national security by designating the Secretary of Commerce as the person responsible to monitor and regulate all export activities related to the transfer of sensitive personal data. It empowers the Secretary to update the list of "high-risk" countries based on need and gives a much-needed legal mechanism to block personal data transfers affecting national security interests.

Should the bill become law, one issue that might arise is the effectiveness of the expanded export regulation. Given that the internet provides an easy mechanism to transfer data quickly abroad, the Senate bill may have limited practical effect in cases where threat actors surreptitiously export or import sensitive personal data to hostile nations without a license. Although the Senate bill targets personal data transfers arising out of commercial transactions, there is a need to address non-commercial activities, including foreign-sponsored espionage operations targeting sensitive personal data of individuals in the U.S.

Attorneys serve an anonymous defendant using an NFT

On June 6, 2022, attorneys from Holland & Knight (Plaintiff's Counsel), a multi-national law firm, served an anonymous defendant by minting a Non-Fungible Token (NFT) and sending it to the defendant's cryptocurrency address. *See https://2no.co/LCXAGService #1 [Etherscan]*, available here. NFTs are digital tokens that commonly represent ownership of unique items. *Non-fungible tokens (NFT)*, available here. Although NFTs are used most commonly to trade "ownership" of digital assets often existing outside the blockchain, the Plaintiff's Counsel used the NFT as the means for service of process to notify the defendant of a pending lawsuit. *LCX [Twitter]*, available here ("First time in history and important for Legal and Crypto Industry as a whole: a temporary restraining order (TRO) to a defendant had been served via NFT . . . .").

Holland & Knight's "service NFT" stems from the pending litigation arising out of a cryptocurrency hack of LCX (also known as the Liechtenstein Cryptoassets Exchange), a Liechtenstein-based fintech providing crypto-asset services. In January 2022, LCX suffered a cyber attack, where an unknown threat actor stole allegedly $8 million worth of cryptocurrencies from one of the company's managed cryptocurrency wallets. *LCX Hack Update*, available here. After discovering the crypto heist, the company engaged with blockchain tracing specialists and also law enforcement agencies in Liechtenstein, Ireland, Spain, and the U.S.

Blockchain investigations revealed that stolen funds were processed initially using a cryptocurrency mixer service that attempts to launder stolen cryptocurrencies to make it difficult to trace the stolen funds. Afterward, the threat actor sent part of the stolen funds to a fully verified user account at Coinbase Europe, one of the major cryptocurrency exchanges that are regulated in Ireland. The threat actor exchanged other parts of the stolen funds with the USD Coin, a stablecoin that is managed by the Centre Consortium, a consortium founded by Circle (a fintech focusing on digital currency) and Coinbase.

Working with law enforcement and prosecution agencies of Ireland and Liechtenstein, LCX was able to obtain a court order to freeze the stolen funds sent to the Coinbase account. The company also retained Holland & Knight to file a complaint against the threat actor in the New York Supreme Court's Commercial Division. The complaint identified the threat actor's cryptocurrency addresses that held the exchanged stable coins and the rest of the stolen cryptocurrency.

With respect to the remaining stolen cryptocurrency, there are no other methods to proactively seize the funds because those funds are fully controllable by the threat actor. To attempt to isolate the threat actor's funds, LCX publicly advised the major blockchain analytics companies of all known addresses controlled by the threat actor and announced that LCX would continue to monitor the stolen funds.

From the legal front, LCX was required to serve the unknown threat actor with service of process. New York State's rules on service of process do not explicitly allow an electronic service to persons. The state did approve new rules allowing New York *businesses* to receive service of process electronically starting January 1, 2023. *New York approves new options for electronic service of process*, available here. For serving individuals, however, an electronic process is permitted only by court order if traditional methods of delivering paper court documents are not applicable or practical. *New York Consolidated Laws, Civil Practice Law and Rules - CVP § 308. Personal service upon a natural person*, available here. Given that one of the threat actor's addresses still had recent transaction activity, serving the threat actor via a special crypto NFT may have been the most reasonable method to satisfy the service of process requirement under New York State's Civil Procedure.

Although serving a defendant via crypto token has not been done before, on June 2, Justice Andrea Masley of the New York State Supreme Court's Commercial Division at New York County ordered Plaintiff's Counsel to serve the defendant via an NFT sent to the defendant's cryptocurrency address. *Order to Show Cause and Temporary Restraining Order, LCX v. John Doe Nos. 1-25*, available here. On June 6, Elliot A. Magruder, a Holland & Knight's attorney, sent the service of token to one of the threat actor's cryptocurrency addresses. *Attorney Affirmation of Service*, available here. The token contained a hyperlink to a URL shortener service that tracks the IP addresses of visitors and redirects them to the Plaintiff Counsel's webpage containing submitted court documents, including the copy of the court order requiring the defendant or an assigned attorney to appear. *See https://2no.co/LCXAGService #1 [Etherscan], supra; see LCX AG vs. John Doe Nos. 1-25 [Holland & Knight]*, available here.

Justice Masley also issued a Temporary Restraining Order (TRO) that legally prohibited the threat actors' ability to transfer or utilize monetary, crypto, or other assets. The TRO was

forwarded to the Centre Consortium, which resulted in the Consortium freezing the USD Coin stable coins held by the threat actor's address. *Etherscan Transaction Details*, available here.

Surprisingly, on June 15, an attorney from the Sharova Law Firm (Defendant's Counsel), which serves the New York and New Jersey area, gave notice of appearance to the court as counsel for the cryptocurrency address holder that has been targeted by the court's TRO. *Notice of Appearance, Sharova Law Firm*, available here. Through its court filings, the Defendant's Counsel challenged the service of proceedings through the crypto NFT. *Affirmation in Opposition to OSC for TRO*, available here. Specifically, the Defendant's Counsel asserted that the Plaintiff's Counsel "failed to follow the court's mandate with regards to service." *Id.* at 4. In response, the Plaintiff's Counsel submitted its own court filings that documented its procedures to serve the defendant via the crypto token in line with Justice Masley's service order. *Affidavit of Andrew W. Balthazor*, available here.

Given that both parties are represented by counsel, the court will likely proceed to the next stage of the litigation. *See generally County Clerk Minutes*, available here.

Analysis

Despite the Defendant's Counsel allegation that the Plaintiff's Counsel failed to adhere to the court's instruction on serving the defendant via a crypto NFT, court and blockchain records indicate that proper procedures likely have been implemented for the service of process. Given that the defendant retained counsel after receiving the service token at his cryptocurrency address (as well as his stable coins being frozen by the Centre Consortium), this particular service of process may have been successful in its goal of notifying the unknown defendant.

It should be emphasized that it has not been conclusively established yet whether the address holder of the seized cryptocurrency address is the same as the threat actor that stole crypto assets from LCX. Although it is clearly established that the threat actor used a cryptocurrency mixer service to launder crypto assets, the burden is on the Plaintiff's Counsel to establish that the identified cryptocurrency addresses received stolen LCX's crypto assets. Specifically, an affidavit submitted by a cryptocurrency laundering tracing expert bases her conclusions on moderate to high likelihood, instead of conclusive determinations, to identify suspect cryptocurrency addresses linked to the threat actor. *Affidavit of Jonelle Still* at 13-14, available here. It is possible that additional evidence may be required, including using discovery procedures, for LCX to successfully litigate its claims of crypto theft against the defendant.