United States v. John Stuart
21-CR-07-LJV-JJM

Defendant's Exhibit D

The case involves a group of investigations and proceedings relating to the sexual exploitation of children on the *Deep Web.* In the investigation, conducted by the Federal Public Prosecutor's Office and approximately twelve police forces from around the world (United States, United Kingdom, Australia, Canada, New Zealand, Germany, Portugal, Italy, Norway, France and Austria), it was possible to verify the activity of a large transnational criminal group, primarily focused on committing the crimes of the sale, dissemination, production and storage of child pornography (Article Nos. 240, 241, 241-A and 241-B of the ECA (*Estatuto da Criança e do Adolescente* [Child and Adolescent Statute])) and rape, including the vulnerable (Article Nos. 213 and 217-A of the Criminal Code), occurring at least since 2013 in *Deep Web hidden services*.

The primary goal of the *Deep Web* is to protect the identity of users by circulating data through a distributed network of computers called nodes. This results in covering up the *Internet protocol (IP),* which is essential for identifying cybercriminals in the most common of investigations. In addition to covering up the *IP* addresses of individual users, the TOR network also allows one to hide the physical location of various *internet* services, forming so-called [bilingual text] *(hidden services).*Such characteristics greatly increase the difficulty of criminal prosecution.

In this case, said hidden services were known by the suggestive names of *Baby Heart, Boy Vids* 4.0, *HurtMeh,* BR Prohibited Angels and *Loli Lust.* In addition, users of these forums totaled 1,839,831 members, from various nationalities and languages of the world, such as German, Chinese, Arabic, Hungarian, among others, who shared and published infant-juvenile sexual abuse content, from photos and videos to rape manuals. The platforms had the following key features:

a) *Baby Heart* (“baby’s heart”, in free translation): designed for the sexual abuse material of infants and children from 0 to 5 years of age;

b) *HurtMeh* (“hurt me”, in free translation): designed for the sharing of images and videos of the sexual abuse of children with an emphasis on *hurtcore* material (sexual abuse with violence), including sadism, torture and the death of children;

c) Prohibited Angels: dedicated to the sharing of sexual abuse material of boys and aimed exclusively at Portuguese speakers;

d) *BoysVids4.0:* designed for the sharing of sexual abuse of boys; and

e) *Lolilust* (something such as "lolita lust", in free translation, alluding to the book "Lolita", by Russian writer Vladimir Nabokov): intended for the sharing of images of the sexual abuse of girls.

The arrest in 2017, in Portugal, of one of the directors of the abovementioned *Baby Heart* led to an investigation in which evidence emerged that led to the arrest and accusation, in Recife/Pernambuco State (PE), of another of its directors.

During the final phase of the proceedings, the Federal Public Prosecutor's Office (MPF, *Ministério Público Federal*) was contacted for a plea bargain agreement with this local administrator, who reported having a direct relationship, through *Deep Web,* with the possible maintainer of several hidden services of child pornography, one of the most sought-after targets in the world by criminal repression agencies. The MPF confirmed, through contacts with the *Federal Bureau of Investigation* (FBI), the existence and importance of this person. According to the FBI, he maintained approximately 70% of child pornography content throughout the *Deep Web* worldwide. So, the MPF signed the plea bargain.

Once the plea bargain agreement was approved, authorization for police infiltration on the *Internet* was obtained, with police agents, the Federal Public Prosecutor's Office and the plea bargainer. The plea bargainer's role was to provide relevant information on common terms among criminals of the hidden services and to make direct contact with the maintainer of the criminal services in order to obtain data for their identification.

The deepening of the contact with the maintainer of the services during the infiltration and technical assistance, legally authorized with the FBI, led to the identification of the *IP* address of the target.

From the IP, registration data was requested from the *internet* service provider. The respective subscriber was a systems analyst who worked with application and web hosting service providers, a profile compatible with the person investigated.

The main suspect certainly had a lot of computer knowledge, because he was able to maintain child pornography services since 2013, which caused additional difficulties for the investigation. Indeed, in this scenario, very possibly all equipment was encrypted, accessible through passwords of great complexity and easily deleted, even from a distance. Therefore, it was necessary to gain access to those still in operation and capture the administrator passwords in order to facilitate forensics and identify the enrolled users. As many of the users claimed and even posted unprecedented images of abuse, discovery of their identity could lead to the rescue of victimized children and adolescents.

Again, with court authorization, lifting of the secrecy and interception of the flow of communications in the computer and network systems of the *internet* access points of the residence of the maintainer of the *hidden services* was conducted.

In the network interception, with the support of the English NCA, the entire data flow of the investigated party was monitored, via unprecedented investigative means in Brazil. It was concluded that, of the 445 GB total analyzed, approximately 374.108 GB (85.53%) corresponded to TOR traffic and that the high daily average of data indicated that the target computer of the intercept acted as a server or *relay* (routing third-party traffic), not as a mere client or user.

In view of such new evidence, the Federal Public Prosecutor's Office obtained authorization for: a) controlled action; b) telephone interception at the terminals of the investigated party or persons associated therewith; c) obtaining of content stored at an *email* provider and *internet* applications; d) ambient capture at the residence, in order to facilitate the recording of passwords when entered by him; and e) search and seizure, including exploratory, at his residence.

The second period of network interceptions was marked by the use of a deanonymization technique (anonymization, inherent to the *Deep Web*) with assistance by the FBI. This police force generated signals to simulate high-volume access to the *hidden services* possibly maintained by the principal person investigated. Thus, after intercepting the address connection, it was possible to distinguish between the periods of normal traffic received by the *hidden service* and the periods during which the signal was sent by the application. The increase in the volume of accesses, simulated by the signal generated, corresponded to the increase in the volume of intercepted data. Thus, the technique corroborated the maintenance of services at the residence.

There was also the telephone interception of numbers associated with this investigated party, which proved useful because dialogs were captured between him and the *internet* provider reporting that the service was not working. During this period, the *hidden services* remained offline; accordingly, criminal liability was reinforced.

The exploratory search, a first-of-its-kind technique that consisted of authorization to enter the target's home, in their absence, in order to analyze the possibility of installing ambient capture cameras (idea subsequently discarded), using a capture device for data typed or transmitted by the *mouse* (*keylogger* and *mouse logger*) and copying data from electronic equipment, also yielded noteworthy results.

On 3/8/2019, the circuit breaker panel of the condominium in which the maintainer resided was accessed. Thus, the electrical power of the property was switched off, leading to the *hidden services*, which were *online* just before the outage, going offline. On 3/12/2019, a new exploratory search found several computers, external and internal HDs, *pen drives* and other media, adopting the decision to copy as much data as possible in the future.

On 6/5/2019, a second exploratory entry was made at the residence, during which *keyloggers* were installed inside two keyboards. With this technique, expertise passed on by the English police, all data entered by the investigated party would be captured and stored. Among this data, the administrator passwords of the forums were key. The occasion was also used for a complete copy of the server's hard drive, temporarily unprotected, for further expert examination in the event of the subsequent destruction of the equipment or ineffectiveness of the *keyloggers.*

After installing the *keyloggers* inside the two keypads, a power outage was again forced for all the servers, so that the investigated party would need to restart these and enter their passwords, now capturable. The strategy worked.

On the following day, 6/6/2019, the preventive arrest warrant and search and seizure warrants were served, making it possible to seize various storage media at the investigated party's residence, some even in operation.

These media were copied and expertly investigated in order to support the continuation of investigations into child abusers in Brazil and around the world, since there was a court authorization to share the material.

In this material, there were 2,042,408 files of sexually explicit or pornographic scenes of children or adolescents. Files were also found referring to the abovementioned *hidden services,* only accessible due to the capture of passwords via the *keyloggers.*

Other means of proof, such as the lifting of *email* secrecy, bank secrecy and tax secrecy, the [ERB] of his cell phone and data from his use of the Uber app, in addition to the physical monitoring of the investigated party when outside his home, proved useful in the instrumentalization of the exploratory search and in the corroboration and discovery of crimes.

Sharing with other countries, for example, led to the release of a boy, abducted and abused for almost two months in Russia, and to various investigations and proceedings in Brazil and elsewhere in the world.

Furthermore, NCA produced reports with the connection *logs* and *IPs* of 68 users of the forums in Brazil, perpetrators of crimes such as rape of the vulnerable and the production, disclosure and acquisition of photographs and videos containing explicit or pornographic sex scenes involving a child or teenager. Among these are criminal agents prosecuted for crimes of the same kind. Evidence regarding the potential maintainer of new child pornography forums is also highlighted.

The deepening of the investigation in relation to these 68 new criminal agents, in an investigation ongoing before the 36th Federal Court of Pernambuco by association, led to a new phase of the operation, with the lifting of identity secrecy, 8 preventive arrests and 105 search and seizure warrants.

Deployment of this new phase, on 12/3/2021, resulted in the serving of all 8 preventive arrest warrants and 23 arrests *in flagrante delicto* for crimes under Art. 241-B of the ECA. Preliminary analysis of the seized equipment led to [the discovery of] new crimes at least under Arts. 240 of the ECA and 217-A of the Criminal Code. Moreover, it allowed for the rescue of 3 children who were victims of possible sexual abuse. The evidence supports further investigations and proceedings in a range of courts.

Finally, I emphasize that there was judicial authorization for the "disclosure regarding the existence of the operation, the proceedings and the facts relating thereto, provided that it is not subsequently possible to identify the victims and those investigated."