

CRIMINAL COURT OF THE CITY OF NEW YORK
COUNTY OF NEW YORK

THE PEOPLE OF THE STATE OF NEW YORK

-against-

Kenneth Kurson (M 46),

Defendant.

FELONY

ADA Alona Katz



Thomas Mullin, Shield #145 of the DISTRICT ATTORNEY OFFICE, states as follows:

The defendant is charged with:

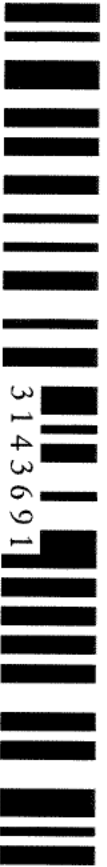
- 1 PL 156.10(1) Computer Trespass
(defendant #1: 1 count)
- 2 PL 250.05 Eavesdropping
(defendant #1: 1 count)

At the times and places described below in the County and State of New York, the defendant, without authorization, knowingly used a computer or computer service with an intent to commit and further the commission of a felony; the defendant unlawfully engaged in wiretapping or mechanical overhearing of a conversation, or intercepting an electronic communication;

The factual basis for these charges are as follows:

From my review of records provided by Awareness Technologies, I know that it is the parent company of WebWatcher, an electronic monitoring software program that, once installed on a target device, enables a user to surreptitiously observe the activity on the target device. The monitored activity includes but is not limited to: keystroke records, websites visited, websites searched, social media activity, and keyword alerts. I have visited www.webwatcher.com and I have viewed the following disclaimer under the terms and conditions: "By accepting this agreement, you agree to only install this software on a device or devices owned by the user. User also agrees to inform any person(s) who uses a device with the software installed of the presence of the software. Failure to comply may result in you breaking state and federal laws."

I have reviewed records from Awareness Technologies pertaining to a WebWatcher account that was purchased by the defendant on September 24, 2015 and subsequently activated on a laptop computer belonging to a person known to the District Attorney's Office ("Individual 1"). As described in more detail below, I believe the computer belonged to Individual 1



CRIMINAL COURT OF THE CITY OF NEW YORK
COUNTY OF NEW YORK

THE PEOPLE OF THE STATE OF NEW YORK

-against-

Kenneth Kurson (M 46),

Defendant.

FELONY

ADA Alona Katz



based in part on the following: the computer was named “[Individual 1]’s Computer,” and I have reviewed correspondence in which Individual 1 describes the computer as belonging to her. My investigation has revealed that Individual 1 and the defendant were married and cohabitating during this time. WebWatcher records list the defendant’s full name, home address in New Jersey, and an AOL email address and phone number registered in his name. WebWatcher records show that the defendant’s WebWatcher account was active and had numerous logins between September 24, 2015 and March 3, 2016. IP addresses collected by WebWatcher show that on November 19 and November 23, 2015, the defendant logged into his WebWatcher account using IP address 162.221.84.15. Records from Single Digits, Inc. show that on these dates, IP address 162.221.84.15 was registered to Observer Media Group, located at 321 W 44th Street in New York County. My investigation has revealed that during this time period, the defendant was employed as the Editor-in-Chief at Observer Media Group.

Based on my review of records obtained from the Federal Bureau of Investigation (“FBI”) and conversations with FBI Special Agent Emily Eckstut, I know that in 2018 the defendant was the subject of a federal background check. During the course of its background check, the FBI learned that the South Orange Police Department (“SOPD”) in New Jersey possessed records pertaining to the defendant’s intrusion into Individual 1’s computer and electronic accounts.

I am informed by a second person known to the District Attorney’s Office (“Individual 2”) that during the summer of 2015, Individual 2 worked with Individual 1 at a summer camp. They became friends and continued to correspond over Facebook and email in the fall of 2015. WebWatcher records associated with the defendant’s account show that the defendant added keyword alerts for variations of Individual 2’s first name. I am informed by Special Agent Eckstut that in October 2015, the director of the summer camp received an email with copies of private Facebook chats between Individual 1 and Individual 2 that took place in September 2015. Based on these facts, I believe that the defendant was using WebWatcher to monitor Individual 1’s online activity, including Individual 1’s communications with Individual 2, without Individual 1’s consent.

WebWatcher records indicate that between September 24, 2015 and November 24, 2015, the defendant logged in numerous times and repeatedly contacted WebWatcher customer



CRIMINAL COURT OF THE CITY OF NEW YORK
COUNTY OF NEW YORK

THE PEOPLE OF THE STATE OF NEW YORK

-against-

Kenneth Kurson (M 46),

Defendant.

FELONY

ADA Alona Katz
[REDACTED]

service when he encountered technical problems or wanted reassurance that his monitoring would not be detected on Individual 1's computer, to which he referred as his "daughter's laptop." For example, on September 25, 2015, the defendant inquired about how to see Facebook content from Individual 1's computer. The defendant wrote: "... I seem to be getting some stuff, but I can't read any of it. For example, I see that my daughter is going on Facebook, but I thought I'd be able to read what she actually wrote? . . . But where can I see the CONTENT of what she wrote? It's not helpful to only see that she went to Facebook – I need to see what she wrote when she was there." WebWatcher customer support then advised the defendant that this data is found under the "Keystroke" category on his account.

On October 17, 2015, the defendant contacted WebWatcher chat support at least four times inquiring whether WebWatcher software could be detected by the user of a device. He wrote that he did not have Individual 1's computer in front of him and inquired how to disable the software. At 6:56 pm, he queried, "Like if someone at the Apple Store is LOOKING for it, will they be able to find it?" At 7:05 pm, he wrote, "I need to uninstall webwatcher from the target Mac. It is not in front of me right now. I need to uninstall it PERFECTLY. So that not even an expert can detect that it had been there." At 7:56 pm, he wrote, "So my question is this: the person who owns the target mac is about to take it to the Mac store. Will they find that the software is on it?" Finally, at 9:21 pm, he asked WebWatcher customer support, "If the person who has the target mac suspects that keystroke software has been installed, am I better off: a) risking being caught uninstalling it? or b) having the target be taken to the apple store and just hoping they don't catch it? . . . So even if the target says to the kid at the Genius Bar 'I think keystroke software may have been installed,' I'm still safe just leaving it alone."

Records obtained from AOL show that in October 2015 the defendant sent himself three emails from the same email account he used to register WebWatcher software. On October 18, 2015, two emails were sent. The body of the two emails read, "[REDACTED]" and "[REDACTED]" respectively. On October 28, 2015, one email was sent with body text that includes, "[Individual 1's first initial and last name]@[Individual 1's employer].org [REDACTED]" Based on the content of these emails, I believe these are Individual 1's passwords, which were obtained through the defendant's use of the WebWatcher software.

Records obtained from a private investigator known to the District Attorney's Office show

3143691

CRIMINAL COURT OF THE CITY OF NEW YORK
COUNTY OF NEW YORK

THE PEOPLE OF THE STATE OF NEW YORK

FELONY

-against-

Kenneth Kurson (M 46),

ADA Alona Katz
[REDACTED]

Defendant.

that on October 20, 2015, Individual 1 emailed the private investigator and reported that the defendant had gotten Individual 2's email address by breaking into Individual 1's email account.

Records obtained from SOPD show that on October 28, 2015, Detective Ernesto Morillo of SOPD interviewed the defendant and Individual 1. According to Detective Morillo's report, they both expressed concern about an unknown actor who had accessed Individual 1's Facebook account without permission. They also reported receiving letters from an anonymous sender that included printed transcripts of Individual 1's private Facebook conversations.

In addition to Detective Morillo's October 28 interview, other evidence indicates that Individual 1 suspected her private correspondence on her computer was being monitored without her permission. On November 3, 2015, Individual 1 sent an email to her contacts asking them to stop using her Gmail account, stating, "Someone has been reading my gmail since the end of October."

Individual 1 took steps to try to detect and remove any unauthorized software running on her computer. Records obtained from SecureMac.com, Inc. show that on November 16, 2015 at 6:44 pm, Individual 1 purchased SecureMac, a security software designed to detect malware on Apple computers. WebWatcher records show that on November 16, 2015 at 8:28 pm, the defendant contacted WebWatcher customer support and asked, "My daughter (who has the target computer) bought 'securemac.com' . . . And also downloaded a program called 'little snitch' that promises to defeat stuff like webwatcher." The defendant asked if WebWatcher would be detected and WebWatcher support stated that it would not be.

On November 24, 2015, Individual 1 reported to SOPD that her husband (the defendant) was "terrorizing her through email and social media causing her problems at work and in her social life." She also reported that the defendant had gained access to her private email account and Facebook account, and created a fake email account in the name of Individual 2 that he had used to send emails.

Apple records show that Individual 1 contacted Apple multiple times to complain that her computer was crashing and that her account password had been changed without her



CRIMINAL COURT OF THE CITY OF NEW YORK
COUNTY OF NEW YORK

THE PEOPLE OF THE STATE OF NEW YORK

-against-

Kenneth Kurson (M 46),

Defendant.

FELONY

ADA Alona Katz



permission. Apple records show that on November 25, 2015, Individual 1 took her Macbook computer to the Genius Bar at the Apple Store located [REDACTED] in [REDACTED] and reported that her computer had been compromised. Genius Bar records show that the computer was examined for malware and two suspicious programs were removed from her Macbook.

False statements made in this written instrument are punishable as a class A misdemeanor pursuant to section 210.45 of the Penal Law, and as other crimes.

Thomas S Mullin #145
Thomas Mullin

8/18/2021
Date

11:05 Am
Time

