GREGORY P. STONE (State Bar No. 78329)
gregory.stone@mto.com
JEREMY K. BEECHER (State Bar No. 301272)
Jeremy.beecher@mto.com
MUNGER, TOLLES & OLSON LLP
350 South Grand Avenue, Fiftieth Floor
Los Angeles, California 90071-3426
Telephone: (213) 683-9100
Facsimile: (213) 687-3702

CAROLYN HOECKER LUEDTKE (State Bar No. 207976)
carolyn.luedtke@mto.com
MUNGER, TOLLES & OLSON LLP
560 Mission Street, Twenty-Seventh Floor
San Francisco, California 94105
Telephone: (415) 512-4000
Facsimile: (415) 512-4077

Attorneys for Plaintiff Intel Corporation

ALTO LITIGATION, PC
Bahram Seyedin-Noor (Bar No. 203244)
bahram@altolit.com
Daniel Sakaguchi (Bar No. 222722)
daniel@altolit.com
Bryan Ketroser (Bar No. 239105)
bryan@altolit.com
Monica Mucchetti Eno (Bar No. 164107)
monica@altolit.com
4 Embarcadero Center, Suite 1400
San Francisco, CA 94111
Telephone: (415) 779-2586
Facsimile: (866) 654-7207

Attorneys for Defendant Doyle Rivers

UNITED STATES DISTRICT COURT

EASTERN DISTRICT OF CALIFORNIA

SACRAMENTO DIVISION

INTEL CORPORATION,

Plaintiff,

vs.

DOYLE RIVERS, an individual, and DOES 1 through 10, inclusive,,

Defendant.

Case No. 2:18-cv-03061-MCE-AC

JOINT STATUS REPORT TO COURT PURSUANT TO FEBRUARY 19, 2019, FEBRUARY 26, 2019, MARCH 4, 2019 AND MARCH 14, 2019 ORDERS

Judge: Hon. Morrison C. England, Jr.
Crtrm.: 7

Plaintiff Intel Corporation ("Intel") filed a motion for a preliminary injunction against Defendant Doyle Rivers ("Rivers"). The Court heard oral argument on February 7, 2019 from counsel for both parties. The Court issued an order on February 19, 2019 (Docket No. 36) that contained a temporary restraining order and an order outlining in detail an inspection that the Court held Intel is entitled to do of Rivers' home computer and any smart printers connected to his home computer (the "Order"). In that Order, the Court asked the parties to submit a status report to the Court on February 21, 2019 outlining the status of the inspection and the need, if any, for a preliminary injunction. On February 21, 2019, March 1, 2019, and March 11, 2019, the parties provided joint status reports and stipulated proposed orders extending the temporary restraining order to March 1, 2019, March 11, 2019 and March 19, 2019, respectively. On March 14, 2019, the Court signed a stipulated proposed order that extended the temporary restraining order to March 19, 2019 and ordered the parties to provide a joint status report on that date. (Docket No. 43).

The parties now jointly submit this further status report and inform the Court that the forensic inspection of Rivers' home computer and smart printers is complete. The parties describe the results of the forensic inspection below. The parties further inform the Court that Rivers has agreed to stipulate to the entry of a preliminary injunction for the pendency of the litigation. The parties submit a proposed order with this status report.

I. JOINT REPORT REGARDING STATUS OF FORENSIC INSPECTION

Rivers turned over his personal computer and several printers to Intel's forensics vendor, Stroz Friedberg, as ordered, on February 8, 2019. Stroz Friedberg then followed the protocol for first preserving the data on the computer and then running searches on the computer. Stroz Friedberg's forensic examination is now complete.

A. Intel's Summary

Intel's inspection of Rivers' personal computer, through Stroz Friedberg, revealed very troubling evidence of wrongdoing by Rivers.

The Court will recall that Rivers resisted the inspection of his home computer, arguing that it was burdensome, invasive, and unnecessary. (ECF No. 12 at 8.) With the Court's

encouragement at the February 7, 2019 hearing, Rivers' counsel ultimately agreed to allow the inspection. As the evidence set forth below outlines, Intel now understands why Rivers resisted inspection of his home computer. The evidence uncovered by Stroz Friedberg reveals that Rivers took great measures to destroy evidence to cover his tracks after downloading confidential and trade secret Intel information, and he then misrepresented his actions in the briefs and declarations filed with this Court. The inspection has uncovered his duplicity.

On October 2, 2018, Intel's in-house counsel sent Rivers a letter outlining Intel's specific concerns about his downloading of trade secret and confidential Intel files to a USB device on September 4, 2018 and September 9, 2018 before he resigned from Intel on September 10, 2018. (Declaration of Carolyn Hoecker Luedtke in Support of Intel's Motion for Preliminary Injunction, ECF No. 10-2, ¶ 2, Ex. A.) In that letter, Intel clearly and unambiguously communicated – with italics, bold and underlining – that Rivers should not take any steps to destroy or alter evidence related to the Intel documents on that device. (Id.) Specifically, Intel instructed Rivers to not "destroy or delete any Intel material that has been transferred," and asked that he "immediately provide access to Intel of the devices and/or the accounts used to download Intel information." (Id.)

Rivers did not return the USB device as requested. He instead gave it to his new employer, Micron. (Id. ¶ 3.) When Micron's counsel eventually agreed to provide it to Stroz Friedberg for analysis, it had been deleted. In pleadings and declarations with the Court, Rivers avoided explaining how or when the USB device had been deleted. (*See generally* Opposition to Motion for Preliminary Injunction, ECF No. 22; Declaration of Doyle Rivers in Opposition to Motion for Preliminary Injunction, ECF No. 22-2.) At the February 7, 2019, Rivers' counsel said the reason for the deletions was "unknown." (Hearing Tr. 18:2-7.)

Rivers' counsel told Intel that the USB device was deleted on Rivers' home computer. As a result, Intel sought an inspection of the home computer to see what it could learn about the deletion of the USB device, whether other Intel confidential files had been transferred to the home computer from the USB device, and whether there was any other evidence on the home computer of what, if anything, additional was misappropriated by Rivers.

The forensics inspection of the home computer was revealing. Stroz Friedberg uncovered evidence that Rivers employed ***six*** different anti-forensic applications on his home computer and USB device designed to permanently delete and encrypt data and to conceal internet activity. These anti-forensic applications were not part of a pattern of activity for Rivers over time. Instead, they appear to be tools that he employed in the wake of his departure from Intel and with increased frequency after Intel raised concerns with him about his taking confidential and trade secret information. It is Intel's view that the evidence of anti-forensic activity raises alarm bells that Rivers was taking steps to destroy evidence of his wrongdoing so that it would not be discovered by Intel.

Specifically, Stroz Friedberg found that Rivers employed the following anti-forensic applications:

- "Eraser" is a "secure data removal tool" whose website promises that it "allows you to completely remove sensitive data from your hard drive by overwriting it several times with carefully selected patterns."[1] Stroz Friedberg found that Eraser was accessed on Rivers' home computer numerous times in October 2018, first on October 16, 2018 – two weeks after Intel's letter regarding the downloaded files – and then again on November 7, 2018. Stroz Friedberg found no evidence that Eraser was installed or run on the computer prior to Rivers' departure from Intel in September 2018.

- "EraserPortable" is a version of "Eraser" specifically designed work on removable storage devices.[2] Stroz Friedberg found EraserPortable was accessed on September 10, 2018 – Rivers' last day at Intel and the day that Stroz found evidence that the SanDisk Cruzer USB drive was connected to his home computer – and again on January 5, 2019, at which time Intel's motion for preliminary injunction and application for expedited discovery was pending. Stroz found no evidence that EraserPortable was installed or run on the computer prior to September 10, 2018.

- "PCShredder" is an application that allows users to "permanently delete files, folders and make them irrecoverable, completely shredding the files you specify, make it impossible for anyone to restore deleted information!"[3] Stroz Friedberg found that PCShredder's last modified date is October 16, 2018, again two weeks after Intel's letter to Rivers. Stroz found no other evidence of PCShredder usage.

- "CCleaner" is an application which removes unused files from a hard drive and cleans traces of users' online activity, such as internet history. Stroz Friedberg found CCleaner was accessed on September 18, 2018 and then on numerous occasions between December 15, 2018 and January 20, 2019. Stroz Friedberg

[1] https://eraser.heidi.ie, visited on March 15, 2019.

[2] https://portableapps.com/apps/security/eraser-portable, visited on March 15, 2019.

[3] http://www.pcshredder.com, visited on March 15, 2019.

found no evidence that CCleaner was installed or run on the computer prior to September 18 2018.

- "Truecrypt" is an application used for "on-the-fly" encryption. Stroz Friedberg found Truecrypt was accessed on September 18, 2018, November 9, 2018 and January 11, 2019. Stroz Friedberg found that TrueCrypt was installed before September 2018 but had never been run before that month.

Stroz Friedberg also found an executable application called "TOR Browser" saved in Rivers' Download folder. While Stroz was unable to find evidence that this program was actually installed, the presence of program on his computer is troubling. Its main purpose is to hide the IP address of the user's computer, as well as to hide the search history of the user. The TOR Browser website states[4]:

- Tor Browser uses the Tor network to protect your privacy and anonymity. Using the Tor network has two main properties:
    - Your internet service provider, and anyone watching your connection locally, will not be able to track your internet activity, including the names and addresses of the websites you visit.
    - The operators of the websites and services that you use, and anyone watching them, will see a connection coming from the Tor network instead of your real Internet (IP) address, and will not know who you are unless you explicitly identify yourself.
    - In addition, Tor Browser is designed to prevent websites from "fingerprinting" or identifying you based on your browser configuration. By default, Tor Browser does not keep any browsing history. Cookies are only valid for a single session (until Tor Browser is exited or a New Identity is requested).

In addition to these anti-forensic applications, Stroz Friedberg found the following:

- *Evidence of mass file deletion:* Stroz Friedberg found that files on Rivers' hard drive had been selectively wiped. Stroz Friedberg was unable to identify what files existed in those locations previously because of the various anti-forensic tools that have been run on the computer by Rivers prior to inspection.

- *Removable storage devices*: Stroz Friedberg identified 14 removable storage devices that have been connected to Rivers' home computer since September 2018. The USB device that Intel has identified to this Court as being used to download material from Rivers' Intel laptop was connected to his home computer on September 10, 2018. In his portion of this Joint Statement below, Rivers has agreed to provide voluntarily eight of these 14 removable storage devices for inspection, but not six removable storage devices Rivers characterizes as fitness activity tracking devices or music devices. Intel reserves the right to seek inspection of those devices as its investigation continues.

[4] https://tb-manual.torproject.org/en-US/about/, visited on March 18, 2019.

- *Potential Intel files*: Using key word searches and MD5 hash values, Stroz Friedberg located a handful of files that Intel believes may potentially comprise confidential Intel files.

- *Cloud storage*: Stroz Friedberg found evidence of a Dropbox account in use but did not find evidence showing Intel files were transferred from Rivers' computer to, or deleted from, the Dropbox account. It is unclear to Intel whether evidence was not available of transfer because of the various anti-forensic tools deployed by Rivers.

- *Email:* Stroz Friedberg likewise found no evidence of data exfiltration via email. It is unclear to Intel whether evidence was not available on transfer because of the various anti-forensic tools deployed by Rivers.

- *Printing:* Stroz Friedberg did not find evidence of printer activity. It is unclear to Intel whether evidence was not available on transfer because of the various anti-forensic tools deployed by Rivers.

- *Browsing history for anti-forensic searches*: Stroz Friedberg did not locate evidence that Rivers searched for ways to download or use anti-forensic tools. Given, however, the accessing of "CCleaner" as well as the presence of the TOR Browser installation applications, both of which remove internet history, Intel cannot know whether this is because Rivers did not run searches on how to destroy documents or whether that evidence has been destroyed by the anti-forensic tools he found through such searches.

Stroz Friedberg has been sharing its analysis with Rivers' counsel as the analysis is complete. Faced with this irrefutable evidence of file wiping and evidence destruction, Rivers had to admit in his recent discovery responses to more wrongdoing than he would admit prior to the inspection. Rivers' recent discovery responses following this forensic inspection are notable.

(1) ***Additional Files Downloaded***

The Court will recall that Intel presented evidence in its motion for a preliminary injunction that Rivers had downloaded an "OrgTree" spreadsheet containing confidential information regarding *thousands* of Intel employees and this was the subject of the Court's inquiry of Rivers at the February 7, 2019 hearing. *See* Hearing Tr. at 11:16-21 ("THE COURT: . . . Why did your client take a thumb drive and download this information? . . . If you tell me because he wanted to send goodbye letters or emails to people, that's ridiculous. Okay. I mean, the court is not stupid here."). Intel also presented evidence in its motion for preliminary injunction that its forensics examiner saw indicia of other downloading on September 4, 2018 and September 9, 2018, but without the USB drive (unavailable because Rivers erased it before turning it over to

Intel), Intel could not identify the names of the documents that were transferred. (Declaration of Michael Hanada, ECF No. 10-5, ¶¶ 8-9.)

In response, Rivers argued to the Court that Intel's motion for preliminary injunction contained only "speculation" about downloading other files. (*See, e.g.*, Opposition to Motion for Preliminary Injunction, ECF No. 22, at 6 ("Intel relies on the innocuous files that Rivers saved to a USB drive in order to speculate—without facts—that Rivers may have also taken trade secret or confidential information.").) Rivers went on to talk about how he purportedly used the "OrgTree" spreadsheet to send a goodbye email and he described his downloading and use of that one file – not mentioning any other files being downloaded. (Id. at 1.)

Intel argued to the Court in response that Rivers' silence in his declaration as to whether he downloaded other files was deafening. (Reply in Support of Motion for Preliminary Injunction, ECF No. 23, at 1.) The Court agreed. (*See* Hearing Tr. 17:2-5 ("I mean, he is -- his silence is deafening in his declaration. It is deafening as to what he doesn't say.").

Rivers provided verified discovery responses on March 11, 2019 that confirm that Intel's "speculative" concerns (concerns that he challenged in front of this Court just a month earlier) about his downloading of other files on September 4 and September 9 were well-founded. Rivers revealed to Intel in his March 11 interrogatory responses that on those two dates, he downloaded to the USB device **three other Intel files: "FocalDetails.xls," "DPM Calc" and "ECC Calc."**[5] He described "FocalDetails" as a file he downloaded "to have a list of the individuals on his team in case he needed to send a farewell email from his personal email account."[6] (This download was *in addition to* the spreadsheet containing a list of thousands of employees' names and contact information about which the Court inquired at the preliminary injunction hearing.) He described "DPM Calc" as "a tool for calculating system fail rates."[7] And he described "ECC Calc" as "a tool for calculating uncorrectable bit error rates."[8]

---

[5] *See* **Exhibit A** at Interrogatory Response Nos. 1 and 2.

[6] *See* **Exhibit A** at Interrogatory Response No. 2.

[7] *See* **Exhibit A** at Interrogatory Response No. 2.

[8] *See* **Exhibit A** at Interrogatory Response No. 2.

Further investigation by Intel has determined that the first file in question, which is actually named "Focal_DSHB_Detail1.xlsx," contains confidential *salary and bonus* information for 31 Intel Non-volatile Memory Solution Group employees – including employees Intel believes Rivers recruited to and hired at his new employer in violation of his non-solicitation agreement. Notably, this file does *not* contain email addresses for those employees. Thus, it would not have served his purported intended purpose to send a goodbye email to his colleagues, as he has claimed. Furthermore, Intel's investigation has revealed that the second file in question, "DPM Calc," which is actually named "dpm_calc_sheet," is a highly sensitive document that is a proprietary tool for running calculations but that also contains highly sensitive and confidential data pertaining to Intel SSD ("Solid State Drive") products that are still under development and have not yet been released. This data includes both technical information as well as sales assumptions and internal product names. Rivers' misappropriation of this file is particularly troubling because these are the precise products Rivers worked to develop at Intel and that Rivers was apparently hired by Micron, a direct marketplace competitor to Intel, to develop there.

Stroz Friedberg did not find these confidential Intel files on Rivers' home computer, likely because of the plethora of anti-forensic programs Rivers ran on his computer before turning it over to Stroz Friedberg for inspection. For the same reason, Intel cannot ascertain whether these highly confidential files have now been transferred to another source. The use of more than a dozen removable storage devices and the extensive anti-forensic effort to cover-up evidence raises serious red flags that Rivers has stowed these confidential files elsewhere and that there is a serious risk that he could continue to access and use them.

2. *Deletion of Misappropriated Files from the USB Device*

Rivers confirms in his interrogatory responses that between October 6, 2018 and October 10, 2018 – *after receiving* Intel's October 2, 2018 letter regarding his misappropriation, in which Intel asked Rivers not to destroy any Intel files on the device and to return it to Intel – he deleted the "OrgTree'" spreadsheet as well as the "FocalDetails.xls," "DPM Calc" and "ECC Calc" files

from the USB device.[9] In this remarkable admission, Rivers does not attempt to explain why he would delete confidential Intel files days after receiving a letter from Intel's counsel communicating in unambiguous terms that he was not to delete any such file and instead was to return the USB device immediately (which he did not do).

3. *Anti-forensic Wiping Of His Home Computer*

Rivers confirms in his interrogatory responses that he ran three different anti-forensic programs identified by Stroz Friedberg's investigation – CCleaner, Eraser and PCShredder – on his personal desktop computer after receiving Intel's October 2, 2018 letter.[10] He states that he used these anti-forensic programs between October 6 and 10, 2018 "in the ordinary course . . . to wipe unallocated space on his personal desktop computer."[11] However, the forensic inspection revealed that the use of these tools was a new activity for Rivers – there was no evidence of using anti-forensic tools prior to downloading documents from Intel onto a USB drive and joining Micron. It is thus unclear how this was done in the "ordinary course."

B. Rivers' Summary

Rivers' produced his home computer for inspection and analysis by Stroz Friedberg, as ordered. Stroz Friedberg examined various forensic artifacts that could indicate a user's interaction with software applications, but which in many instances were inconclusive. For example, where certain forensic artifacts may indicate that a software application was opened or viewed, but not that it was run or executed, the most that can be said regarding that application was that it was accessed. In some instances, an executable application was present, but there was no indication that it had been installed on the computer. Other forensic artifacts permitted Stroz Friedberg to determine conclusively that the software application had been run, and in some instances, to state what actions that it took.

---

[9] *See* **Exhibit A** at Interrogatory Response Nos. 7-8.

[10] *See* **Exhibit A** at Interrogatory Response No. 18.

[11] *Id.*

Additional removable USB devices: The USB device that Intel has identified to this Court as being used to download material from Rivers' Intel laptop was connected to his home computer between October 6-10, 2018. Stroz Friedberg identified 14 additional removable USB devices, including eight storage devices, four fitness activity tracking devices and two music devices that have been connected to Rivers' home computer since September 2018. Rivers has agreed to produce the storage devices to Stroz for inspection as soon as practicable.

Searches for Intel files: Using MD5 hash values, Stroz Friedberg located only the 110 Perl Scripts that Rivers created while he was an employee of Micron during the time period from 2006-2009. With additional keyword searches, Stroz Friedberg identified over approximately 2,593 documents, of which well over 2,500 Stroz Friedberg deemed to be "false positive" hits. Stroz Friedberg found 19 unique text messages (and copies thereof, totaling 51 text messages) that contained keyword hits. These files were provided to counsel for Rivers for further review, and none were determined to contain Intel confidential information. Stroz Friedberg also found six unique files (and copies thereof totaling 12 files) that contained keyword hits. These files were provided to Rivers' counsel for review, where it was determined that the files date back to approximately 2006. The files contain the words "Intel Confidential" within them, however they do not contain any Intel Confidential information. Notwithstanding the foregoing, Rivers agreed that Intel may remediate and remove these files from his computer.

Cloud storage: Stroz Friedberg found evidence of a Dropbox account in use but did not find evidence indicating that any Intel files were transferred from Rivers' computer to, or deleted from, the Dropbox account.

Email: Stroz Friedberg found no evidence of data exfiltration via email.

Printing: Stroz Friedberg did not find evidence of printer activity.

Browsing history for anti-forensic searches: Stroz Friedberg did not locate evidence that Rivers searched for ways to download or use anti-forensic tools.

No Mass file deletion: Stroz Friedberg found no evidence of mass file deletion immediately prior to the time that the computer was forensically imaged, but could not state that the free or unallocated space of the computer had not been wiped in recent months. In the

execution log that Stroz Friedberg located for the Eraser program (see below), Stroz Friedberg found that the only task listed for the program was to wipe free or unallocated disk space and file slack. Stroz Friedberg also found patterns of file removal that were consistent with the automated cleaning activity that the CCleaner application (see below) was configured to perform upon startup.

Stroz Friedberg's forensic inspection showed that Rivers installed or accessed some software applications on his home computer and USB device that clean and optimize computer hard drive space and registries and ensures internet browsing privacy, which are capable of making deleted files unrecoverable, as well as securely wiping files. Specifically, Stroz Friedberg found that Rivers had the following applications or installation files on his computer:

- "CCleaner" is a computer utility program used to optimize computer performance, clean potentially unwanted files and invalid registry entries from a computer and protect internet browsing privacy, and is capable of making deleted files unrecoverable and securely wiping files. Stroz Friedberg found CCleaner configured to be run upon the computer's startup, with certain cleaning functions, including removal of internet cookies, to be performed automatically. Stroz Friedberg's forensic analysis indicated that CCleaner was installed on October 20, 2018 and last run on January 20, 2019.
- "Eraser," is an application capable of making deleted files unrecoverable, as well as securely wiping files. According to Stroz Friedberg's findings, Eraser was used on October 17, 2018 only to wipe the computer disk's free or unallocated space along with file slack.
- "EraserPortable" is also an application capable of making deleted files unrecoverable, as well as securely wiping files. Stroz Friedberg found that EraserPortable was accessed on September 10, 2018 – Rivers' last day at Intel. Stroz Friedberg's analysis shows that EraserPortable was accessed on January 5, 2019, however Stroz Friedberg did not conclude that it had been used to securely wipe any files.

- "Truecrypt" is a file encryption application, which Stroz Friedberg found to have been installed several years ago—in 2015. Stroz Friedberg's analysis showed that Truecrypt was accessed in some way on September 18, 2018, November 9, 2018 and January 11, 2019.
- "PCShredder" is also a tool capable of making deleted files unrecoverable, as well as securely wiping files. Stroz Friedberg found a copy of the installation file for PCShredder in Rivers' downloads folder, with a last-modified date of October 16, 2018, however Stroz found no indication that PCShredder had been installed or run.
- Stroz Friedberg also found an executable application called "TOR Browser"—a web browsing application that protects users' identities online, and can hide a user's IP address—saved in Rivers' Download folder. Stroz found no indication that this program was actually installed or used.

II. PARTIES' POSITIONS REGARDING ENTRY OF PRELIMINARY INJUNCTION

Rivers has agreed to stipulate to a preliminary injunction in this matter. Therefore, the parties are jointly submitting a proposed stipulated preliminary injunction for the Court's review. If the Court would like additional supporting information, the parties are of course available to provide that information to the Court at any time.

Specifically, the proposed stipulated preliminary injunction will (1) enjoin Rivers from possessing, using or disclosing any confidential, proprietary, or trade secret Intel documents related to 3D XPoint or Intel's Optane™ branded products, including about Intel personnel working on those products, that he acquired while working for Intel and that contain information Intel has not disclosed outside of Intel except under a nondisclosure agreement protecting its confidentiality; and (2) order Rivers to return to Intel within three business days all confidential, proprietary or trade secret Intel documents related to 3D XPoint or Intel's Optane™ branded products, including about Intel personnel working on those products, that he acquired while working for Intel and that contain information Intel has not disclosed outside of Intel except under a nondisclosure agreement protecting its confidentiality.

DATED: March 19, 2019

Respectfully submitted,

MUNGER, TOLLES & OLSON LLP

By: */s/ Carolyn Hoecker Luedtke*
CAROLYN HOECKER LUEDTKE
Attorneys for Plaintiff Intel Corporation

DATED: March 19, 2019

ALTO LITIGATION, PC

By: */s/ Daniel Sakaguchi*
DANIEL SAKAGUCHI
Attorneys for Defendant Doyle Rivers

ECF ATTESTATION

I, Carolyn Hoecker Luedtke, am the ECF user whose account is being used to file this document. In accordance with Civil Local Rule 5-1(i)(2), I attest that concurrence in the filing of this document has been obtained from all signatories.