U.S. Department of Justice

United States Attorney

Eastern District of Pennsylvania

Robert J. Livermore
Direct Dial: (215) 861-8464
Facsimile: (215) 861- 8618
E-mail Address:robert.j.livermore@usdoj.gov

615 Chestnut Street
Suite 1250
Philadelphia, Pennsylvania 19106-4476
(215) 861-8200

July 12, 2016

The Honorable Joel H. Slomsky
United States District Court
Eastern District of Pennsylvania

Re: U.S. v. Yu Xue, et al.
16-CR-22
Response to Defendant's July 1, 2016 Letter and Proposal

Dear Judge Slomsky:

I am in receipt of the defendants' proposed solution to the discovery protective order which was filed with the Court in a letter dated July 1, 2016. As described below, the defendants' proposal is not a viable plan.

Before addressing the defendants' proposal, the government would like to address some common themes the defendants have raised both in their July 1, 2016 letter and in other pleadings. Obviously, the defendants are trying to convince the Court that they have not committed any crime and that the discovery materials at issue do not warrant the protections sought by the government. The facts alleged in the indictment prove otherwise. The defendants are charged with stealing highly valuable materials which the government intends to turn over in discovery. As alleged in this indictment, these materials relate to biopharmaceutical products which typically cost more than $1 billion to research and develop. Thus, the materials to be turned over in discovery are extraordinarily valuable, contrary to the defendants' representations to the Court.

The indictment specifically alleges that the defendants stole 23 documents that contain trade secret and other confidential material. These 23 documents referenced in the indictment are only the tip of the iceberg. During the course of the government's investigation, the FBI executed search warrants over various e-mail accounts used by the defendants and seized numerous other documents that contain trade secret and/or confidential material. Although not referenced in the indictment, this does not make these materials any less valuable. In addition, on January 2016, the FBI arrested the four defendants and executed additional search warrants. This evidence seized was also not part of the first indictment. In these searches, especially of the electronic devices, the FBI found a treasure trove of additional evidence relating to the defendants' fraud schemes. For example, on defendant TAO LI's computer, the FBI found

entire folders of highly valuable research data stolen by defendant YU XUE. The amount of data stolen was quite extensive. For the defendants' to suggest that the defendants' fraud scheme was limited in nature is simply not supported by the evidence.

Furthermore, as alleged by the indictment and as the government will prove beyond a reasonable doubt at trial, the defendants' motivation for stealing these items was pecuniary. They intended to resell the stolen information in China for a substantial profit. They created a company in China called Renopharma to market and sell the stolen information. The government's evidence will show that for some of the stolen documents, the defendants' simply removed the "GSK" label and added a "Renopharma" label in order to market and sell the stolen information in China. The seized e-mail records prove that the defendants' attempted to sell this data to third parties in China. The seized e-mails showed that the defendants' believed that they would reap huge financial profits from selling the stolen information. Unfortunately, the FBI does not have the ability to investigate Renopharma's criminal conduct in China. Small portions of Renopharma's financial records were seized in the e-mail search warrants. These records show substantial sums of money being deposited into the Renopharma accounts from various sources, including the government of China. The money laundering conspiracy charged in this case relates to the defendants' efforts to hide the proceeds of the fraud in the names of family members in China and elsewhere, demonstrating the defendants' knowledge and intent in implementing their nefarious schemes. For the defendants to suggest that the stolen documents have never been "disseminated" is completed refuted by the evidence as the defendants are charged with that very conduct.

The government's evidence at trial will prove that the defendants are thieves who stole an immense amount of material with the intention of selling this highly valuable information for profit in China, and they plotted to hide their ill-gotten gains in the names of family members in China. For these reasons, the defendants are extreme risks to continue this course of conduct while preparing for trial. The government is not speculating that the defendants' might steal this information, the government will prove that they have already stolen it once and there is no reason to believe that they would not do so again. None of the defendants are presently working. The criminal prosecution has obviously put enormous financial pressure on the defendants and there will be great temptation to attempt to profit from this information as they attempted to do so in the past.

Compounding this problem is the fact that co-defendant YAN MEI is a fugitive. The government believes that he is presently in China working for Renopharma along with other Renopharma employees. The government further believes that Renopharma continues to attempt to market and sell the stolen information. YAN MEI and Renopharma provide a ready outlet for the defendants to ship any additional information they wish to steal at this juncture. The discovery materials could be transmitted to YAN MEI in a number of different forms including e-mail, text messages, or other types of communication with little chance of detection. This fact heightens the risk of continued theft.

Under the law, the Court is required to protect trade secrets "to the fullest extent" for

prosecutions involving theft of trade secrets. Hsu v. United States, 155 F.3d 189, 197 (3d Cir. 1998). In many trade secret cases, the trade secret material never leaves the FBI office. The defendants must come to the FBI office to view this material. Here, due to the volume of information at issue, the government is willing to make some concessions to ensure that the defendants have adequate opportunity to prepare for trial. The government has proposed several viable options for the defendants to review this material, all of which have been rejected.

In response, the defendants have offered their own proposal. As the government understands the defendants' proposal, the defendants would agree that the government could install one security camera in each defendant's house. The security camera would be focused on the area of the home where the defendant will be performing his or her document review. The government would have the right to remotely monitor the cameras in real time. The defendants would have the discovery materials on a stand-alone computer. The computer (and any notes that the defendants take) would remain in the camera's line of sight at all times. In addition, the government would be permitted to take an image of the standalone computers to audit and inspect the defendants' use thereof at the government's convenience.

Unfortunately, the defendants' proposal falls far short of the Hsu standard for several different reasons.

1. First and foremost, the government simply does not have the resources to devote to monitor four cameras, 24 hours a day, 7 days a week, in perpetuity in order to effectively enforce the protective order. That monitoring activity totals 35,040 monitoring hours per year. It only takes an instant to snap a photograph or otherwise violate the Court's order. The Court has not set a trial date in this matter. The government would expect that a realistic trial date would be at least one year from now. An FBI agent typically works around 2000 hours per year. Therefore, the defendants' proposal would require a team of 18 agents devoting 100% of their time monitoring the computers remotely looking for a needle in a haystack. This is not a situation where an agent could watch the video in fast-forward or spot check because they would likely miss the needle as it passed. Thus, it would impossible for the FBI to effectively monitor the cameras to ensure compliance with the Court's order.

2. Second, one camera cannot adequately cover all necessary angles to ensure compliance with the Court's protective order. Either the defendants or third parties could easily take a photograph of the discovery materials outside of the camera range without the monitoring agents observing the infraction.

3. Third, the cameras do not provide any security against third parties unlawfully accessing the discovery materials by stealing the laptop. The government is equally concerned with third parties stealing this data as it is with the defendants' themselves further compromising this material. The defendants' homes are unsecure locations. Their home addresses are now a matter of public record. This case has already received a considerable amount of media attention (even on routine discovery matters) and the government is deeply concerned that third parties may attempt to steal this very valuable information.

4. Fourth, cameras are relatively rudimentary technology. Cameras can be manipulated or bypassed by a number of techniques which the government would not be able to adequately monitor. Furthermore, cameras are susceptible to malfunction through ordinary wear and tear, power outages, network outages, and a host of a number of other reasons. Therefore, cameras do not provide adequate security for this highly valuable material.

5. Fifth, the defendants' proposal that the government image and audit the stand alone computers in the defendants' homes provides no succor. The discovery hard drives will contain at least one, possibly several, terabytes of data. It typically takes the government weeks to image and analyze that immense amount out of data. To ensure the integrity of the data, the government would have to image the computers at least several times per month. The end result is that the government would be required to have four teams of agents for year or probably longer doing nothing other than imaging the hard drives, analyzing the results, and looking for the needle in the haystack. The government does not have four teams of computer technicians available for that type of work. Moreover, the government would have to save each and every image. By the end of this case, the government would be storing hundreds of terabytes of data at immense cost in both time and money. After the fact monitoring would also not prevent the defendants from stealing the data in the first instance.

Finally, the defendants' proposal does not consider a number of logistical and legal impediments to placing a video camera inside the defendants' homes. There are a number of other agencies, including the Department of Justice, Office of Enforcement Operations, the U.S. Marshals Service, and Pretrial Services, which also may have to approve placing video cameras in the home. Placing a video camera inside a defendants' home is not as simple as they make it appear. The government avers that the serious constitutional implications emanating from the government installing cameras in the home are far more compelling than a scheduled visit from a security guard. Under applicable law, the government would need written consent to videotape from all occupants of the home. All visitors to the home would, at a minimum, be required to be alerted to the presence of the video cameras. The government would also need written consent to enter the defendants' home 24 hours a day, 7 days a week, to service the cameras as needed and ensure that the cameras are functioning properly.

In fact, many of the defendants' concerns over the government's security guard proposal are equally or more problematic than the defendants' camera proposal. First, the defendants' object to the government's security guard proposal because "it would require the defendants to accommodate a stranger (and potentially multiple strangers over time) in their homes, potentially at all hours of the day and night." This is exactly what would happen under the defendants' own proposal. FBI agents and contractors would be allowed to enter their home at any time of day to check the camera and computer. Second, the defendants' characterize the government's security guard plan as setting a "dangerous precedent" which "seriously implicates the defendants' constitutional rights." The defendants' arguments here are nonsensical. The defendants do not object to government agents entering their home at any hour of the night or day for unscheduled monitoring but do object to private security guards entering their home for appointments which

they schedule at their own convenience. There can be no constitutional violation for a private person entering the defendants' homes when they have a scheduled appointment.[1]

Some of the defendants' objections will be non-issues. The defendants express concern over the timing of appointments. One of the main advantages of hiring security firms is that a security guard will be available whenever the defendants' wish to schedule an appointment. If the defendants do not wish to "accommodate a stranger after hours or on weekends," they do not have to do so. The defendants' can schedule appointments when it is convenient for them. The government believes this is an improvement over the Court's plan of hiring an attorney whose availability will likely be more limited. In a similar fashion, the defendants' concern about communicating privately with counsel is equally unwarranted. The defendants can simply step away from the computer and speak to counsel in private. There is nothing about the government's plan which would interfere with their ability to contact counsel.

In sum, the defendants' proposal neither provides the necessary security for the discovery materials nor is the proposal logistically feasible. The government maintains that the "security guard" proposal previously submitted provides both the necessary security features and allows the defendants to review the discovery from the convenience of their own homes.

Respectfully Submitted,

ZANE DAVID MEMEGER
United States Attorney

/s/
Robert J. Livermore
Assistant United States Attorney

cc: Peter Zeidenberg, Esq.
Counsel for YU XUE

John Josephs, Esq.
Counsel for TAO LI

David Schertler, Esq.
Counsel for TIAN XUE

Eric Yaffe, Esq.
Counsel for LUCY XI

[1] The defendants' arguments make it seem as if they have never hired a contractor to fix their air conditioning or a leaking faucet. Virtually everyone invites "strangers" into their home on a routine basis for a variety of reasons. To suggest that this conduct is inappropriate defies convention.