2008 WL 11230384
Only the Westlaw citation is currently available.
United States District Court, C.D. California.

UNITED STATES of America, Plaintiff,
v.
Tien SHIAH, Defendant.

CASE NO. SA CR 06-92 DOC
|
Signed 02/19/2008

Attorneys and Law Firms

Lawrence E. Kole, AUSA - Office of US Attorney, Santa Ana, CA, for Plaintiff.

James D. Riddet, Bienert Miller and Katzman PLC, San Clemente, CA, Thomas Joseph Nolan, Nolan Armstrong & Barton LLP, Palo Alto, CA, for Defendant.

FINDINGS OF FACT AND CONCLUSIONS OF LAW

DAVID O. CARTER, United States District Judge

***1** Pursuant to Defendant Tien Shiah's ("Shiah") waiver of his right to a jury trial, this criminal case was called to trial before this Court without a jury on September 11, 2007. The matter was taken under submission by the Court on October 19, 2007 after eleven days of trial, consisting of opening statements, witness testimony, stipulations on evidence and submission of evidence, and closing arguments. Plaintiff, the United States of America (the "Government") submitted a closing trial brief and Shiah submitted proposed findings of fact and conclusions of law. The Court, having heard all of the testimony and considered all admissible evidence, as well as the arguments of counsel, Shiah's proposed findings of fact and conclusions of law, and the Government's closing trial brief, hereby enters its Findings of Fact and Conclusions of Law.

FINDINGS OF FACT

A. Shiah's Life Prior to Broadcom

Shiah was born in Taiwan and moved to Canada at an early age. He attended the University of British Columbia, where he obtained a bachelor's degree in applied science in 1990. Shiah also received a master's degree in business administration from McGill University in 1997. His first employment in the United States was with Conexant in Southern California, where he was employed from 1998 until January 2001. At the time, he was in the process of receiving an adjustment of immigration status to legal permanent resident. He had previously resided in the country on a work visa. Shiah accepted a job with Broadcom Corporation ("Broadcom"), a semiconductor company, in September 2000, but he did not actually begin work until January 2001 on the advice of his immigration attorney, so as not to delay immigration proceedings.

Shiah gave two weeks notice of his departure from Conexant. Prior to his departure, Shiah gathered many of the files and documents that he had accumulated during his employment with Conexant. In Shiah's view, the files and documents were a "toolkit" that he kept as a record of his work, a practice which he believed to be in line with common industry practice and his previous habits in academia. Shiah believed that some of the information would have been considered confidential by Conexant at the time he departed. Shiah's "toolkit" from Conexant included a laptop that he had previously used at the company, which contained all of the files that he had downloaded to that computer before receiving a new laptop, as well as hard copies of other files. In sum, there were several hundred files in Shiah's Conexant "toolkit."

B. Shiah's Employment at Broadcom

Shiah began employment with Broadcom on January 12, 2001 as a Product Line Manager ("PLM") in the ethernet marketing group, a group responsible for Broadcom's high-speed ethernet products. In summer 2003, there were two other PLMs in Shiah's group: Gregory Youngblood ("Youngblood") and Vinod Lakhani ("Lakhani"). Greg Young ("Young") was the director of marketing for ethernet products and the direct supervisor of the three PLMs. The PLMs had several primary job responsibilities, including selling Broadcom's ethernet products to customers and developing new ethernet products. Broadcom's three primary customers were Dell, IBM, and Hewlett–Packard ("HP"), accounting for approximately 70 percent of the ethernet group's total revenues. When Shiah began work as a PLM, he was responsible for both Dell and IBM, although Youngblood took responsibility for domestic IBM in early 2003. Lakhani was responsible for HP, and Shiah retained responsibility for Dell. Shiah was also responsible for the entire Asian market until leaving the company.

***2** When Shiah started work at Broadcom on January 12, 2001, he signed a document entitled "Statement Regarding Confidentiality and Invention Assignment Agreement" ("Confidentiality Agreement"). *See* Exhibit 18. The Confidentiality Agreement was provided by an individual in human resources, and Shiah recalls reviewing the document for a couple of minutes before signing it. Shiah does not recall ever seeing it again during the course of his employment at Broadcom or being given a copy of the document after signing it. In addition, Shiah was never given clarification regarding the contents of the Confidentiality Agreement.

The Confidentiality Agreement defined "Confidential Information" to include "all information that has or could have commercial value or other utility in the business in which the Company or Clients are engaged or in which they contemplate engaging" and "all information of which the unauthorized disclosure is or could be detrimental to the interests of the Company or Clients, whether or not such information is identified as Confidential Information by the Company or Clients." *Id.* p.2. Examples of Confidential Information were set forth, including

> any and all information concerning teaching techniques, processes, formulas, trade secrets, inventions, discoveries, improvements, research or development and test results, specifications, data, know-how, formats, marketing plans, business plans, strategies, forecasts, unpublished financial information, budgets, projections, and customer supplier identities, characteristics, and agreements.

Id. pp.2–3. By signing the agreement, Shiah agreed "that at all times during or after his or her employment, [he] will hold in trust, keep confidential, and not disclose to any third party or make use of the Confidential Information of the Company or Clients." *Id.* p.3. Furthermore, the Confidentiality Agreement set forth that upon termination:

> Employee agrees, promptly and without request, to deliver to and inform the Company of all documents and data pertaining to his or her employment and the Confidential Information and Inventions of the Company or Clients, whether prepared by Employee or otherwise coming into his or her possession or control, and to sign the Termination Certification attached to this Agreement as Schedule C.

Id. pp.5–6. It also warned of potential civil liability and criminal liability under California state law for the unauthorized taking of trade secrets. *Id*. p.6. The Confidentiality Agreement also stated that the employee will prevent the misappropriation or disclosure of Confidential Information and "will not disclose or use to his or her benefit (or the benefit of any third party) or to the detriment of the Company or its Clients any Confidential Information or Invention." *Id*. p.6. Shiah signed the agreement below a line indicating that he "read this agreement carefully and understands its terms." *Id*. p.8.

Shiah also received a laptop computer from Broadcom at the beginning of his employment ("Broadcom laptop"). Young told Shiah that he could take the laptop off site with him in order to do work.

Shiah never received any education or training from Broadcom regarding what information the company considered confidential. He also does not recall ever having conversations with colleagues regarding confidentiality. Similarly, the other Broadcom employees who testified at trial indicated that they did not recall receiving training or having conversation relating to what information Broadcom considered confidential. Instead, Shiah, like other employees, based his opinions regarding what the company considered confidential on his own common sense. The only instruction Shiah received about when or how to mark documents confidential was that he was told to use the Microsoft PowerPoint company template when producing presentations. The template included the words "Broadcom Proprietary and Confidential" in the footer on each page, causing each page of a presentation to be marked confidential, regardless of the contents of that page. Shiah does not recall being instructed to treat documents, files, or presentations differently based on whether they were to be shared only

within Broadcom or were intended to be distributed to customers and clients.

***3** In Spring 2003, Broadcom conducted an informal peer review of Shiah. Young presented the results to Shiah, which included critical feedback. Specifically, Young indicated that there was a perception that Shiah was not sufficiently familiar with the developing technologies marketed by the PLMs to their customers. In addition, Young explained that Shiah was not adequately following up with customers after they began to implement Broadcom devices in their product. Finally, the review indicated that Shiah needed to be more aggressive in marketing the ethernet products to his customers.

C. Shiah's Departure from Broadcom

After this peer review, Shiah felt that his work was underappreciated, and he began to look for employment elsewhere. On May 15, 2003, a recruiter submitted Shiah's resume to Marvell, a San Francisco Bay Area computer technology company and competitor of Broadcom. *See* Exhibits 25 and 26. Marvell interviewed Shiah on June 12, 2003. *See* Exhibits 28 and 33. On July 14, 2003, Shiah submitted his formal written employment application to Marvell. *See* Exhibit 33. One week later, on July 21, 2003, Marvell offered Shiah a position as director of product marketing. *See* Exhibit 35. Shiah's offer included annual compensation of $150,000, an increase in salary of approximately $50,000 from his employment at Broadcom. The offer also included stock options and $25,000 in moving expenses. In making the offer, Marvell did not request that Shiah bring confidential information from Broadcom, and Shiah did not offer to do so. Shiah accepted the offer from Marvell and indicated that he would start work in Northern California on August 25, 2003, although he did not immediately notify Broadcom that he had accepted the new position. *See* Exhibit 35.

Shiah's delay in notifying Broadcom was influenced by the fact that his Broadcom stock options vested at the end of each month. Thus, he intended to notify Broadcom of his departure in the beginning of August, planning for his last day to be August 12, 2003. On August 4, 2003, Shiah attempted to give Young notice that he was leaving, but Young was out of town. Shiah ultimately met with Young the morning of August 7, 2003. He notified Young that he was planning to leave after August 12, 2003 and gave Young a resignation letter. *See* Exhibit 23. Shiah elected not to tell Young that he was going to Marvell in response to Young's inquiries about where Shiah was going after leaving Broadcom. At the August 7, 2003 meeting Young told Shiah that he could work through August 12. However, the next morning, August 8, Young told Shiah that he would not be permitted to return the following work day. Accordingly, August 8, 2003 was Shiah's final day, but he was still paid through August 12, 2003.

The same day that Shiah submitted his application to Marvell, July 14, 2003, Shiah purchased a Maxtor external hard drive which he intended to use to create a "toolkit" of the files and documents he had accumulated while working at Broadcom. *See* Exhibit 97. Beginning in July 2003, Shiah began to create this "toolkit." During this time period, Shiah received a number of additional documents other than the documents already on his Broadcom laptop. On July 14, 2003, Shiah requested and received Dell presentation.ppt in an email from Dana McCarty, a Broadcom employee. *See* Exhibit 90. On July 24, 2003, Shiah received StdQ303.xls (Indictment File # 1; Exhibit 4) via email, as discussed more fully below. *See* Exhibit 217. A mass email was sent to numerous Broadcom employees, including Shiah, informing the employees that all the presentations from the PC Team Sales Training had been loaded on the Intranet on July 1, 2003. *See* Exhibit 24. Shiah followed up on this email on July 28, 2003, seeking sales presentations on HP, IBM, Gateway, and eMachines. *See id.* On July 30, 2003, Shiah received Palomar Concept Approval rev1.ppt (Indictment File # 2; Exhibit 8) in an email from Lakhani, discussed more fully below. *See* Exhibit 91. On July 31, 2003, Shiah requested and received ROI_V008_PalomarDiablo_concept_approval.xls (Indictment File # 4; Exhibit 7) from Lakhani, as discussed more fully below. *See* Exhibit 94. On the same day, Shiah also sent an email to Youngblood saying, "I would like to review your IBM presentation and follow up with how we want to pitch this at other accounts." *See* Exhibit 95.

***4** On the morning of August 4, 2003, Shiah copied approximately 4,700 files from his Broadcom laptop to the external hard drive. *See* Exhibits 1, 10, and 54. This wholesale transfer of files included every file from the Ethernet folder in which Shiah kept all work-related files that he accumulated while at Broadcom, as well as every email he had sent or received while working at Broadcom. Shiah deliberately copied all files and emails from his Broadcom laptop so that his "toolkit" would include all files and emails related to his work at Broadcom.

Following the wholesale transfer of documents, Shiah made several further attempts to gather and accumulate information to complete his "toolkit." During the afternoon of August 4,

Shiah received an email containing a file entitled Network cc action items 8–04–03.xls (Indictment File # 9; Exhibit 10). *See* Exhibit 93. After receiving the file via email, he copied that file to the external hard drive. *See* Exhibits 93, 99, and 128 line 31503. On August 5, Shiah downloaded five files to the external hard drive from Docsafe, a password protected folder on Broadcom's Intranet that allowed outside customers to access files. *See* Exhibits 1, 54, 99, and 128 lines 30110, 30111, 31575, 32619, 32620, 32621, and 32622. These files related to the 5788 ethernet device, for which Shiah was responsible, and Shiah created a folder titled BCM5788 for four of the downloaded files. *See* Exhibit 129. He copied six additional files to the external hard drive on August 6. These files consisted of two non-Broadcom files from the Internet (MRD_template.doc and Positioning_template.doc), two files related to Fujitsu (wakeuplan_driver_test_item(3).doc and wiredlan_driver_instration_requests.doc), a company for which Shiah was responsible, and two files related to Shasta (Shasta_MRD_Bill_02b.doc and 3GIO_feature_review.ppt), a future product for which Shiah was responsible. *See* Exhibits 1, 13, 54, 99, and 128 lines 34579, 34580, 32085, 32084, 31577, and 31576. Shiah continued to be involved with work related to Fujitsu through the end of his job. *See* Exhibit 247. Shiah added two more Broadcom files to the external hard drive on August 7, 2003. *See* Exhibits 1, 54, 99, and 128 lines 32617 and 32618. After copying these files, Shiah did not take any steps to cover his tracks and hide the fact that he had copied the files, other than deleting files from his computer that one might expect an employee to delete on his last day of work, even though he knew that he would be leaving Broadcom and turning over the laptop to Broadcom. One day after leaving Broadcom, on August 9, 2003, Shiah backed up the majority of files from the external hard drive onto CDs.

On Shiah's last day, August 8, 2003, Youngblood and Lakhani took him out to lunch prior to his exit interview. Shiah's exit interview was conducted by Noel Whitley ("Whitley"), Broadcom's in-house counsel, and an individual from human resources named Naomi Sullivan ("Sullivan"). Whitley was chosen to attend the interview because he was still in the office on Friday afternoon when the interview was to occur. When he met with Shiah, Whitley was supposed to "scare the hell out of" Shiah in regard to taking or disclosing Broadcom's confidential information. At the interview, Whitley informed Shiah that he had been told that Shiah accepted a job with Marvell. This surprised Shiah, as he had previously declined to tell Young that he was going to Marvell. Whitley discussed the importance of protecting Broadcom's confidential information and further informed Shiah that he was forbidden from sharing Broadcom's confidential information at Marvell. Whitley further stated that technical documents were confidential as well as a wider range of business information, such as pricing lists and business road maps. During the interview, Shiah asked Whitley several questions, including what information Broadcom considered to be a trade secret, whether Shiah could work with products in the same market while at another company, and whether it would be a problem if he worked with customers in the future that Broadcom had shared. Whitley declined to answer these questions or give any guidance, instead advising Shiah that he should consult an attorney. In addition, Whitley never stated that Shiah was required to return copies of files on which he had worked while at Broadcom and never asked Shiah whether he had copied files, although he did say that Shiah should get rid of all Broadcom documents before leaving. The Confidentiality Agreement which Shiah initially signed when he arrived at Broadcom, *see* Exhibit 18, was not provided during the exit interview.

***5** Shiah has no recollection of signing Schedule C, which was referred to in the Confidentiality Agreement as the Termination Certification that employees were required to sign upon departure, during his exit interview. The Broadcom Exit Interview Checklist shows that the box next to the Schedule C, Termination Certificate line is marked "Yes." *See* Exhibit 21 p.1. However, the Checklist also contains handwritten language stating, "Schedule C—consult w/ attorney." *See id.* p.2. No copy of Schedule C signed by Shiah was introduced into evidence, and such a document could not be found by the Government. A version of Schedule C, unsigned by Shiah, that was last revised in January 2002 and was executed in November 2003 was provided as an exhibit. The exhibit indicates that the Schedule C was targeted to prevent the conduct alleged in this case, copying and retaining documents. *See* Exhibit 251.

Shiah's first day of work at Marvell was August 25, 2003. His job title was director of marketing for Marvell's ethernet products, and his primary responsibility was to market Marvell's Yukon ethernet product line to customers in the PC market. *See, e.g.,* Exhibit 246. Shiah signed a confidentiality agreement on his first day at Marvell in which he agreed not to "improperly use or disclose any proprietary information or trade secrets of any former or concurrent employer." *See* Exhibit 37 p. 1. Shiah also received a Marvell issued laptop computer.

D. Indictment Documents on External Hard Drive

The documents that Shiah copied to the external hard drive and took with him when he left Broadcom were intended to make up a complete repository of all files and emails related to Shiah's work at Broadcom. The nature of these documents ranged from highly sensitive and confidential information to publicly available information. If the some of the information in these documents were disclosed, competitors would obtain advantages, such as the ability to successfully compete with Broadcom on price, negotiate terms from their suppliers and customers more successfully, and take advantage of Broadcom's research and development. Furthermore, information indicating prices paid by Broadcom to their suppliers, as well as information indicating prices that Broadcom's customers paid, could enable customers or suppliers to negotiate more effectively with Broadcom. Finally, if other entities' confidential information, such as Broadcom customer information, was released by Broadcom, then Broadcom could lose business of those customers. The following section discusses the documents included in this repository that are listed in the Indictment in this case and further discusses how they were originally obtained by Shiah.

1. Indictment File # 1 (Std03Q3.xls), *see* Exhibit 4

Std03Q3.xls is a spreadsheet containing standard cost information for Broadcom ethernet devices. The information contained in Std03Q3.xls was kept and updated by Broadcom employees Verna Lum Ayer ("Ayer") and Emery Chang ("Chang"). The general practice used by the PLMs to obtain necessary information from this document was to request cost information from Chang, either via email or in person, for particular devices with which they were working. The PLMs needed this information so that they could become familiar with the cost information for each product and negotiate a price effectively. This document contains information that Broadcom considered confidential in 2003. In fact, almost all of the information contained in this document would have been confidential information, as it includes internal costs, test and assembly yields, and individual product revenue and margin. In addition, this spreadsheet contains information related to the royalties paid by Broadcom that is kept confidential between Broadcom and the licensor to whom it relates.

Shiah obtained this document while seeking cost information for several devices for which he had responsibility. On July 23, 2003, an employee of Broadcom named Jerry Lee ("Lee") sent Shiah an email stating that he had quoted a price of $23.73 to a customer for the 5700 and 5421 devices, which the customer misunderstood to mean that the quoted price was $23.73 for both of the devices. *See E* xhibit 223 p. 1. Shiah responded to this email that the price quote was incorrect and that each chip had a price of $23.73. *See id.* Shiah went to Chang's office to request cost information for the 5700, 5421, and several other devices for which he had responsibility. Chang sent Shiah an email with attached cost information for the 5700 device on July 24, 2003, at 4:25 p.m., but did not include information for the other requested devices. *See* Exhibit 220. As a result, Shiah went to Chang's office to notify him that the email did not contain all of the requested cost information. At 4:34 p.m. on the same day, Chang sent Shiah an email with a link to a site on the Broadcom Intranet containing folders of cost information, including the file Std03Q3.xls. *See* Exhibit 217. Later that same evening, Shiah accessed the link from the email and copied Std03Q3.xls to the Ethernet folder on his Broadcom laptop. *See* Exhibit 229 p.56 line 2730 column F.

2. Indictment File # 2 (Palomar Concept Approval rev1.ppt), *see* Exhibit 8

***6** Palomar Concept Approval rev1.ppt is a PowerPoint presentation prepared by Lakhani for the ethernet group. The presentation relates to the Palomar product, a new ethernet device that Broadcom was developing in 2003. Lakhani was primarily responsible for developing the Palomar product. However, Broadcom did not produce all of its ethernet products specifically for particular customers. Instead, many of the products were developed for multiple customers, and, thus, pertinent to all of the PLMs. This file contains some information that Broadcom would have considered confidential in 2003. Specifically, the document contained plans for Palomar, information that was particularly sensitive because the product was not then available on the public market.

On July 30, 2003, Shiah received an individual email from Lakhani containing the Palomar Concept Approval rev1.ppt presentation. On August 1, 2003, Lakhani sent an email to a group of Broadcom employees, including the PLMs and Shiah, with the same Palomar Concept Approval rev1.ppt presentation attached. *See* Exhibit 208. It was not an uncommon practice for members of the ethernet group to share information and files regarding products that the group planned to market. Prior to receiving the second email from Lakhani, Shiah had downloaded Palomar Concept Approval rev1.ppt to the Ethernet folder of his Broadcom laptop during the evening of July 30, 2003. *See* Exhibit 229 p.55 lines 2669.

Shiah had previously made at least one presentation to Dell on June 23, 2003, in which he included the Palomar product as part of his sales pitch. *See* Exhibit 224 p.10.

3. **Indictment File # 3 (CA_arch1–0703.ppt)**, *see* Exhibit 9

CA_arch1–0703.ppt is also a PowerPoint presentation prepared by Lakhani for the ethernet group relating to the Palomar product. This presentation also contains some information that Broadcom would have considered confidential in 2003, namely, plans for the unreleased Palomar product.

On July 30, 2003, the marketing manager for the ethernet group, Uri Elzer ("Elzer"), sent an email to a group of Broadcom employees, including the PLMs and Shiah, with CA_arch1–0703.ppt attached. *See* Exhibit 210. Shiah did not request this file. The presentation was downloaded to the Ethernet folder of Shiah's Broadcom laptop during the evening of July 30, 2003. *See* Exhibit 229 p.55 lines 2668.

4. **Indictment File # 4 (ROI_V008_PalomarDiablo_concept_approval.xls)**, *see* Exhibit 7

ROI_V008_PalomarDiablo_concept_approval.xls is a spreadsheet containing the return on investment analysis ("ROI") for the Palomar product, a study relating to the financial feasibility of the product. This document also contains plans for the unreleased Palomar product, information that Broadcom would have considered confidential in 2003.

The morning after Elzer sent Shiah Indictment File # 3, July 31, 2003, at 10:53 a.m., Shiah emailed Lakhani to request that the Palomar ROI analysis be sent to him so he could understand Lakhani's background calculations. *See* Exhibit 94. Three minutes after Shiah's email, Lakhani replied to Shiah and attached ROI_V008_PalomarDiablo_concept_approval.xls to his reply email. *See id.* Shiah subsequently saved the file to the Ethernet folder of his Broadcom laptop. *See* Exhibit 229 p.55 line 2670 column E. He had previously downloaded the same file to the same location on July 22, 2003, although the source from which he previously obtained the file is not contained in the record. *See id.* column F.

5. Indictment File # 5 (Competitive GB Analysis 6–16–03.xls), *see* Exhibit 6

Competitive GB Analysis 6–16–03.xls is a document created by Shiah while employed at Broadcom. It is one of a number of specific projects that Shiah undertook during the course of his employment that related to general aspects of the personal computer market, rather than just aspects pertaining to his specific client. The document contains publicly available information and industry perceptions of Broadcom and its competitors. It also contains information that was considered confidential in 2003 about Palisades, a product that Broadcom had not yet released to the market. This information includes data comparing Palisades to products from three of Broadcom's competitors. Shiah was primarily responsible for developing the Palisades product. *See* Exhibit 232. In addition, the document contains other information that was considered confidential in 2003, including cost information for the 5705 product and pie charts derived from that cost information. Finally, the document contains detailed statistics on the number of gates used to perform various functions, statistics that were not publicly known and could not be determined by reverse engineering. Shiah did not mark any pages of the document to indicate confidentiality.

6. Indictment File # 6 (Tier 1 volumes.xls), *see* Exhibit 2

***7** Tier 1 volumes.xls is a two page document that was also created by Shiah while employed at Broadcom. It contains sales volume information for Dell, HP, and IBM, including information for desktop and laptop computers, and individual products within each category. The aggregate sales information was publicly available. Some of the individual sales volume numbers would have been considered confidential by the individual companies such as Dell. The document also contains internal codenames for products sold by Broadcom's customers which were not generally known to the public. Shiah did not mark the document to indicate confidentiality.

7. Indictment File # 7 (All Designs 7–24–03.xls), *see* Exhibit 3

All Designs 7–24–03.xls is another two page document that Shiah created while employed at Broadcom. The document lists which ethernet devices were being used in which computers, by which customers, including Dell, IBM, HP, Fujitsu, Sun, Apple, and 3Com. The document contains information that Broadcom would have considered

confidential in 2003. It contains internal revision data and sales volume data broken down by individual Broadcom products sold to particular customers, information that was not publicly known. Furthermore, the document also contains internal codenames for products sold by Broadcom's customers which were not generally known to the public. Young and Shiah both indicated that information in this document might have been considered confidential. Shiah did not mark the document to indicate confidentiality.

8. Indictment File # 8 (Rebates 5–27–03.xls), *see* Exhibit 5

Rebates 5–27–03.xls was also created by Shiah while employed at Broadcom. This spreadsheet contains data regarding the rebates Broadcom paid to its customers for ethernet products sold to those customers. Large volume, primary customers, such as Dell were given a rebate from the contract manufacturer average sale price ("CM ASP"). The customers initially paid the CM ASP, but subsequently received a rebate per chip to reduce the actual sale price, called the net average sale price ("Net ASP"). The Net ASP and rebates were negotiated with the respective PLMs. The Net ASP and rebates were information that would have been considered confidential by Broadcom in 2003, particularly due to the fact that there was significant variation between the prices paid by the customers. The rebate information was kept confidential between Broadcom and the particular customer to whom it related. Shiah did not mark the document to indicate confidentiality.

9. Indictment File # 9 (Network cc action items 8–04–03.xls), *see* Exhibit 10

Network cc action items 8–04–03.xls is a regularly updated document containing notes and action items from weekly conference calls with HP, attended by members of the ethernet marketing team. The document was periodically emailed to a group of Broadcom employees who were privy to the details and status of the phone calls. This document was the most recent update as of August 4, 2003. It contains information that Broadcom would have considered confidential in 2003, as well as markings on the action items pages to indicate confidentiality. Some of the confidential information includes notes pertaining to discussions of new products under development by HP and other issues known only to HP and Broadcom. It was attached to an email that Shiah, as well as other Broadcom employees, received on August 4, 2003, at 1:06 p.m. *See* Exhibit 213.

E. Files Accessed by Shiah While Working at Marvell

On several occasions while he was working at Marvell, Shiah accessed some of the files that he had copied onto his external hard drive. There are five known dates that Shiah accessed Broadcom files from the external hard drive after arriving at Marvell. Shiah claims that he had no intention of ever using any of the information contained in any of the files accessed that, in his view, Broadcom would have considered confidential. The following section discusses the files Shiah accessed after starting work at Marvell and the circumstances surrounding the file accesses.

1. September 8, 2003

***8** Shiah accessed five files on September 8, 2003 by connecting the Maxtor external hard drive to his Marvell laptop for several hours during the afternoon. *See* Exhibits 103 and 112 p.1. These files are (1) Competitive GB Analysis 6–16–03.xls (Indictment File # 5) and (2) Tier 1 volumes.xls (Indictment File # 6), as well as three files not named in the Indictment, specifically, (3) 5788 vs Marvell comparison 6–16–03.xls, (4) Competitive Technical 6–18–03.xls (Exhibit 113), and (5) Segment Analysis summary 4–29–03.xls (Exhibit 130). *See* Exhibits 103 and 112. All five of these files were among the approximately 4,700 files that Shiah downloaded from his Broadcom laptop to the Maxtor external hard drive on August 4, 2003. The file 5788 vs Marvell comparison 6–16–03.xls is a document comparing a released Marvell Device to a released Broadcom device. Segment Analysis summary 4–29–03.xls contains summaries of sales volume information for companies in the PC market. *See* Exhibit 130. Competitive Technical 6–18–03.xls is a one page table containing publicly available, non-confidential, information about products released by Broadcom and its competitors. *See* Exhibit 113.

Shiah accessed Competitive GB Analysis 6–16–03.xls (Indictment File # 5), 5788 vs Marvell comparison 6–16–03.xls, and Competitive Technical 6–18–03.xls to produce a chart comparing Marvell to four of its primary competitors as part of his duties as marketing director. The chart is part of a two page document, named Competitive GB analysis.xls, created by Shiah on his Marvell laptop while accessing the external hard drive on September 8, 2003. *See* Exhibits 105 and 112. The first page of Competitive GB analysis.xls is nearly identical to the first page of Competitive GB Analysis 6–16–03.xls (Indictment File # 5; Exhibit 6) and contains information regarding general industry knowledge about the strengths and weaknesses

of five companies, including Broadcom and Marvell. *See* Exhibits 6 and 105. Competitive GB analysis.xls contains no confidential information on the first page. In addition, page two of Competitive GB analysis.xls contains only publicly available information from released products. It is nearly identical to Competitive Technical 6–18–03.xls, with a new Marvell product substituted for the comparison. *See* Exhibits 113 and 105. Thus, these three documents were accessed for the publicly available data they contained in order to generate a document containing only publicly available data.

On the same day that this access occurred, Marvell had a response due to an IBM Request for Quotation ("RFQ") and emailed that response at the end of the afternoon. *See* Exhibits 64 and 114. The response to the RFQ proposed prices of $4.45 and $4.95 for two different Marvell products. Competitive GB Analysis 6–16–03.xls (Indictment File # 5; Exhibit 6) contains a cost breakdown for a competing Broadcom 5705 product and shows the total cost for that product to be $5.54. *See* Exhibit 6 p.10. Shiah denies that he was involved in setting the price on the RFQ, and further states that the cost information contained in Competitive GB Analysis 6–16–03.xls does not overlap with the price information in the RFQ.

Shiah accessed Tier 1 volumes.xls (Indictment File # 6) and Segment Analysis summary 4–29–03.xls in order to view aggregate PC volumes information. His goal was to understand the overall market size in his role as a marketing director.

2. September 12, 2003

On September 12, 2003, Shiah accessed two files located on the Maxtor external hard drive. The two files accessed by Shiah, neither of which are listed in the Indictment, are (1) Japan_2003.ppt and (2) PC_Segment_Offsite_June_12_2001.ppt (Exhibit 14). Both were among the 4,700 files that Shiah copied from his Broadcom laptop to the Maxtor external hard drive on August 4, 2003. Japan_2003.ppt is a document containing a product roadmap. Shiah accessed this document to obtain a template for a product roadmap. The formatting accessed by Shiah was not confidential, but instead consisted of general skills and knowledge. PC_Segment_Offsite_June_12_2001.ppt was a presentation given by the Broadcom marketing team to the sales team, regarding the Gb ethernet product. *See* Exhibit 14. It contained market trends relating to ethernet products, as well as PC market shares and design cycles. *See id.* Shiah accessed this presentation to look at market size information and volumes of top PC vendors. The market information is public information provided by industry analysts.

3. September 16, 2003

***9** Shiah accessed ten files on the Maxtor external hard drive on September 16, 2003. *See* Exhibit 103. These ten files are (1) All Designs 7–24–03.xls (Indictment File # 7; Exhibit 3), (2) Rebates 5–27–03.xls (Indictment File # 8; Exhibit 5), and (3) Network cc action items 8–04–03.xls (Indictment File # 9; Exhibit 10), as well as seven files not named in the Indictment, specifically, (4) 570x Auto Approve, 22 May 03.xls (Exhibit 131), (5) Dell Worksheet for ex 4–22–03.xls (Exhibit 132), (6) Desktop–Wkstn Eng Call—11–20–02.xls (Exhibit 124), (7) Desktop–Wkstn Eng Call—11–27–02.xls (Exhibit 125), (8) Network cc action items 2–24–03.xls (Exhibit 123), (9) New 570x Tactical Forecast 30 July03.xls (Exhibit 11), and (10) Notebook Eng Call –04–07–03.xls (Exhibit 126). *See* Exhibit 103. All ten of these files were among the approximately 4,700 files that Shiah copied from his Broadcom laptop to the Maxtor external hard drive on August 4, 2003, although Network cc action items 8–04–03.xls was copied over individually after the general download, later on the same day.

On September 10, 2003, Shiah traveled to Houston to meet with HP. He returned on September 12. *See* Exhibits 67 and 68. On September 15, 2003, Shiah received an email from Pat Keeley ("Keeley"), a Marvell employee, containing a list of action items to follow up on with HP. *See* Exhibit 68. Keeley asked Shiah for a presentation on Marvell's support model, especially regarding people in place in Taiwan, and stated that HP was not interested in the Marvell Yukon device because of power demands. *See id.* Five of the files accessed on September 16 contained notes of Broadcom calls with HP regarding product issues: Network cc action items 8–04–03.xls; Network cc action items 2–24–03.xls; Desktop–Wkstn Eng Call—11–20–02.xls; Desktop–Wkstn Eng Call—11–27–02.xls; and Notebook Eng Call –04–07–03.xls. *See* Exhibits 10 and 123–126. In addition, Rebates 5–27–03.xls contained Broadcom pricing to HP, All Designs 7–24–03.xls contained information on HP's current and future programs, and New 570x Tactical Forecast 30 July03.xls contained forecasts of future Broadcom business with HP. *See* Exhibits 5, 3, and 11. On September 16, Shiah responded to the HP action item regarding power demands of the Yukon product. *See* Exhibit 69.

Shiah claims that his purpose in accessing all of these files was to find other sources of aggregate volume information

for PC manufacturers as a cross-check. He claims that he was not attempting to look at other information in doing so. When he did not find the information he was seeking in a given file, he then moved on to the next file. Shiah accessed these files prior to a presentation, which he gave two days later on September 18, 2003, about the financial goals of the Yukon ethernet product line. *See* Exhibit 246. The presentation included information about market size, market share, and aggregate volume, the same information Shiah claims to have been seeking when he accessed the ten files on September 16. *See id.* None of the information in this presentation is information that was or would have been considered confidential to Broadcom.

Some of the files accessed by Shiah on September 16 contained aggregate volume information, whereas some of the files did not contain the information Shiah claims to have been seeking. Shiah was unable to tell whether or not the information was contained in the files without opening them or relying on his own recollection. For example, All Designs 7–24–03.xls (Indictment File # 7) contained volume information, although it did not contain the specific volume information Shiah was seeking. *See* Exhibit 3. Dell Worksheet for ex 4–22–03.xls did contain aggregate volume information. Shiah claims that he thought that 570x Auto Approve, 22 May 03.xls, Desktop–Wkstn Eng Call—11–20–02.xls, Desktop–Wkstn Eng Call—11–27–02.xls, Network cc action items 2–24–03.xls, New 570x Tactical Forecast 30 July03.xls, and Network cc action items 8–04–03.xls (Indictment File # 9) might have the information he was seeking, but realized that they did not contain that information after opening them. With respect to Rebates 5–27–03.xls (Indictment File # 8), Shiah claims he thought that the total rebate calculations were included in the spreadsheet, from which he could derive aggregate volume information. This information was not contained in the file. *See* Exhibit 5.

***10** Although Shiah had previously accessed Tier 1 volumes.xls, which contained aggregate volume information, Shiah claims that he was searching for volume information in other files in order to cross-check the information he had already obtained. Furthermore, Shiah's presentation on September 18 contained information for companies other than just those companies listed in Tier 1 volumes.xls (Indictment File # 6). *See* Exhibits 246 and 2.

4. September 17, 2003

On September 17, 2003, Shiah accessed four files located on the Maxtor external hard drive, none of which are listed in the indictment. These files are (1) 5705A0_Power.xls, (2) 5705M_Mini–PCI_railbyrail power_v1p0.pdf, (3) eMachines Acct Review 6–03.ppt (Exhibit 122), and (4) Taiwan support.ppt (Exhibit 17). *See* Exhibits 103 and 112 p.3. These four files were contained among the approximately 4,700 files that Shiah copied from his Broadcom laptop to the Maxtor external hard drive on August 4, 2003.

5705A0_Power.xls and 5705M_Mini–PCI_railbyrail_power_v1p0.pdf contained power measurements for two released Broadcom products. Shiah accessed these files in order to see how the power measurements were formatted, information that is not confidential.

The document eMachines Acct Review 6–03.ppt is a presentation containing, among other information, several organizational charts of officers and executives at eMachines as well as Broadcom's goals for its eMachines customer account. *See* Exhibit 122. Shiah claims that he accessed the file in order to find a contact person at eMachines from the prior contacts he had established while at Broadcom. The Marvell sales team was, at the time, experiencing difficulty organizing a face to face meeting with eMachines. *See* Exhibit 72, p.2. Both Shiah and Youngblood agree that the identity of a contact is not confidential information, but is instead general skill and knowledge.

Finally, Taiwan support.ppt is a presentation that was given to second tier customers to show them how Broadcom planned to support them through Broadcom's product support model and personnel in place in Taiwan. *See* Exhibit 17. It was created by Shiah while he was an employee at Broadcom. Shiah claims that he accessed this file to look at the format of a chart on page 8 of the presentation. He was interested in the format of the slide. He did not consider the format of the slide that he previously prepared to be confidential information. At the time he accessed the file, Shiah was responsible for creating the Marvell presentation regarding Marvell's customer support model, particularly with respect to people in place in Taiwan. *See* Exhibit 68 p.1. Shiah then reported that he sent a Marvell support model to HP during the week ending September 19, 2003. *See* Exhibit 72.

5. September 22, 2003

Finally, the last time that Shiah accessed files on the Maxtor external hard drive while he was employed at Marvell was September 22, 2003. On this day, Shiah accessed three

additional files that are not listed in the Indictment. These files are (1) Dell Org Chart Client.ppt (Exhibit 15), (2) Dell Org Chart.ppt, and (3) Dell presentation.ppt (Exhibit 16). *See* Exhibits 103 and 112 p.3. These three files were among the approximately 4,700 files that Shiah downloaded from his Broadcom laptop to the Maxtor external hard drive on August 4, 2003. Dell Org Chart Client.ppt is a PowerPoint presentation created by Shiah while he was employed at Broadcom. It contains an organization chart of officers at Dell, as well as information indicating Broadcom and Shiah's strategies pertaining to Dell. *See* Exhibit 15. Dell Org Chart.ppt is not an exhibit. Dell presentation.ppt is a Broadcom presentation that provides an overview of Dell as an organization and client of Broadcom. *See* Exhibit 16.

***11** On September 19, 2003, Shiah received an email from David Young, a Marvell employee, asking Shiah to identify "silver" accounts, defined as high volume opportunities that Marvell must win. *See* Exhibit 71. Examples of such accounts included Dell, IBM, HP, Fujitsu, Toshiba, LG, and Samsung. *See id.* David Young said that they needed to set the expectation that sales should invest time to obtain silver account business. *See id.* On September 22, 2003, Shiah received an email from Joe O'Connor ("O'Connor"), a Marvell employee, requesting names of individuals with whom Shiah had relationships in Dell marketing. *See* Exhibit 245 p.3. Shiah accessed the Maxtor external hard drive that evening for 16 minutes. *See* Exhibit 112. Seven minutes after disconnecting the Maxtor external hard drive, Shiah emailed O'Connor to suggest that he try contacting Tim Mattox ("Mattox"), the VP of Marketing at Dell. *See* Exhibit 245 p.3. Shiah accessed Dell Org Chart Client.ppt, Dell Org Chart.ppt, and Dell presentation.ppt during the time he was connected to the Maxtor external hard drive. He accessed Dell Org Chart Client.ppt, which did not contain the Dell contact, before accessing Dell presentation.ppt, which did contain Mattox's name and title on page eight. *See* Exhibits 15 and 16 p.8. Shiah and Youngblood both agree that business contacts established during employment are not information that is confidential to the employer. Shiah sent O'Connor only the name and title of Mattox, and there is no indication that Shiah accessed the three documents for any other purpose than to find the Dell contact, despite the fact that the documents contained additional information.

F. Broadcom's Security Measures

Broadcom was a "fabless" semiconductor company in 2003, which meant that its semiconductor products were fabricated at third party facilities based on designs created by Broadcom. Accordingly, the value of Broadcom's products was derived from the intellectual property contained within their designs. This resulted in some of the documents and information possessed by Broadcom being highly sensitive and confidential, and much of Broadcom's value derived from this confidential information.

In addition to the Confidentiality Agreement discussed above, Broadcom had multiple measures in place in 2003 to protect its trade secrets from persons outside the company. Ken Venner ("Venner"), Broadcom Vice President and Chief Information Officer, testified to a number of these measures. Broadcom's physical facility was protected by a security guard, security cameras, and receptionists who monitored visitors. Doors were kept locked and keycards were required for entry. Furthermore, the servers were maintained at an offsite data center with limited access. As for electronic data, Broadcom had numerous measures in place for protection. For example, Broadcom employed an information technology team, firewalls, file transfer protocols, intrusion detection software, and an extra layer of protection between the internet and the internal system. In addition, passwords were required to access the internal system, and many sensitive files were stored on individual computers rather than shared servers. When outside entities received access to documents or computer files, these entities were required to sign non-disclosure agreements. Shared electronic documents were placed on a separate system called DocSafe. DocSafe tracked usage and data transfer, and it was only accessed through secure password-protected websites provided by Broadcom. Finally, Broadcom marked documents that were shared to outside entities with a legend indicating that they were confidential or proprietary.

In general, Broadcom employees understood the types of information that were considered confidential and should not be disclosed, in contrast to public information. For example, Lakhani, Youngblood, and Shiah, the three PLMs, were all able to identify certain information that was considered confidential and other information that was considered to be public during their testimony. Furthermore, Broadcom employees, including Lakhani, Youngblood, Young, and Venner indicated that Broadcom did not permit its employees to retain confidential documents after leaving the company. The employees repeatedly indicated that Broadcom's corporate culture was one in which confidentiality was valued and protected. Venner explained that Broadcom's concern for security led Broadcom to have a reputation as a company that was stingy with its data.

Broadcom employees also indicated that the files Shiah took contained information related to products sold outside of California and in foreign countries.

G. The Investigation

***12** This case was brought to the attention of the Government authorities pursuant to an investigation conducted by Broadcom after Shiah left. On September 10, 2003, Broadcom submitted a memorandum to James W. Spertus, Assistant United States Attorney, setting forth facts that it believed amounted to probable cause that a violation of 18 U.S.C. § 1832 and other federal statutes had occurred. *See* Exhibit 245. The letter listed files created and accessed by Shiah prior to his departure and set forth information that employees of Broadcom would report if interviewed. *See* Exhibit 245. The letter further stated, "we request that, until we have had an opportunity to discuss this matter, the long list of file names found in this letter not be included in documents that could later become publicly available." Exhibit 245 p.20. It closed by stating, "Broadcom appreciates your immediate attention to this sensitive matter." *Id.*

Although Broadcom did not examine Shiah's computer prior to his departure, Broadcom did investigate Shiah's actions after he departed. Broadcom made a copy of Shiah's hard drive, but did not make a perfect bit by bit image of Shiah's hard drive. After making a copy, Broadcom then re-circulated Shiah's laptop to another employee at Broadcom. Broadcom did not inquire from Shiah whether he had documents in his possession as he departed from the facilities.

The Government authorities relied on information from the Broadcom documentation indicating that files were accessed and deleted from Shiah's Broadcom laptop. The FBI searched Shiah's apartment on September 26, 2003. Approximately five FBI agents came to Shiah's apartment and remained there for approximately four hours. They seized computer media pursuant to a search warrant, including the Maxtor external hard drive and CDs containing approximately 4,700 Broadcom files. Shiah was cooperative when the FBI arrived, and he said that it was common practice for him to keep copies of files from employers and other items from his past, such as college and bank records. He further stated that he deleted files from the laptop as part of cleaning his desk on his last day. He also stated that the copies of files that he saved were for his personal use and that he had no intention to provide them to his new employer. Shiah reiterated during this search that he did not want to defraud anyone.

The Indictment in this action was filed on May 10, 2006 after subsequent investigation by Government authorities, nearly three years after Shiah's last day at Broadcom.

CONCLUSIONS OF LAW

Shiah is charged in a three-count Indictment with violating 18 U.S.C. § 1832(a), the Economic Espionage Act ("EEA"). Count One involves alleged stealing and misappropriation of trade secrets. Count Two involves alleged duplication and copying of trade secrets. Count Three involves the possession of stolen trade secrets. Each of these three counts alleges the corresponding conduct, i.e. misappropriation, duplication, and possession, respectively, in relation to nine particular Broadcom computer files ("Indictment Files"). Only one file containing information qualifying as a trade secret need have been misappropriated, duplicated, or possessed in order to find guilt for each corresponding count. In evaluating whether Shiah had the requisite *mens rea,* the Court can consider evidence of his conduct related to other files copied to the external hard drive and not charged in the Indictment, because that conduct is inextricably intertwined with conduct alleged in the Indictment. *See United States v. Sayakhom,* 186 F.3d 928, 937–39 (9th Cir. 1999).

A. Elements of the Offenses

1. Count One: Stealing and Misappropriating Trade Secrets, 18 U.S.C. § 1832(a)(1)

Count One charges Shiah with stealing and misappropriating trade secrets in violation of 18 U.S.C. § 1832(a)(1). The elements of Count One that the Government seeks to prove beyond a reasonable doubt are the following: (1) Shiah took or carried away without authorization from Broadcom one or more computer data files that contained one or more trade secrets; (2) Shiah knew or had a firm belief that the information in the computer data file or files was one or more trade secrets; (3) the information in the computer data file or files was in fact one or more trade secrets; (4) Shiah intended to convert one or more of the trade secrets to the economic benefit of anyone other than the owner, which may include Shiah himself; (5) Shiah intended or knew the theft would injure the owner of the trade secrets; and (6) one or more of the trade secrets were related to or were included in a product that was produced for or placed in interstate or foreign commerce. *See* 18 U.S.C. § 1832(a)(1).

2. Count Two: Copying and Duplicating Trade Secrets, 18 U.S.C. § 1832(a)(2)

***13** Count Two charges Shiah with copying and duplicating trade secrets in violation of 18 U.S.C. § 1832(a)(2). The elements of Count Two that the government seeks to prove beyond a reasonable doubt are the following: (1) Shiah copied or duplicated without authorization from Broadcom one or more computer data files that contained one or more trade secrets; (2) Shiah knew or had a firm belief that the information in the computer data file or files was one or more trade secrets; (3) the information in the computer data file or files was in fact one or more trade secrets; (4) Shiah intended to convert one or more of the trade secrets to the economic benefit of anyone other than the owner, which may include Shiah himself; (5) Shiah intended or knew the copying or duplication would injure the owner of the trade secrets; and (6) one or more of the trade secrets were related to or were included in a product that was produced for or placed in interstate or foreign commerce. *See* 18 U.S.C. § 1832(a)(2).

3. Count Three: Possessing Stolen or Misappropriated Trade Secrets, 18 U.S.C. § 1832(a)(3)

Count Three charges Shiah with possessing trade secrets that were stolen or misappropriated in violation of 18 U.S.C. § 1832(a)(3). The elements of Count Three that the government seeks to prove beyond a reasonable doubt are the following: (1) Shiah possessed one or more computer data files that contained one or more trade secrets that were taken or carried away without authorization from the owner; (2) Shiah knew or had a firm belief that the information in the computer data file or files had been taken or carried away without authorization from the owner; (3) Shiah knew or had a firm belief that the information in the computer data file or files was in fact one or more trade secrets; (4) the information in the computer data file or files was in fact one or more trade secrets; (5) Shiah intended to convert one or more of the trade secrets to the economic benefit of anyone other than the owner, which may include Shiah himself; (6) Shiah intended or knew the theft and possession would injure the owner of the trade secrets; and (6) one or more of the trade secrets were related to or were included in a product that was produced for or placed in interstate or foreign commerce. *See* 18 U.S.C. § 1832(a)(3).

B. Definition of Relevant Terms

1. "Owner"

The term "owner" means the person or entity who has rightful legal or equitable title to, or license in, the trade secret. 18 U.S.C. § 1839(4).

2. "Trade Secret"

The term trade secret includes "all forms and types of financial, business, scientific, technical, economic or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing." The owner must also have "taken reasonable measures to keep such information secret," and the information must "derive independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public" in order to qualify as a trade secret. 18 U.S.C. § 1839(3).

C. The Economic Espionage Act

The Economic Espionage Act of 1996 ("EEA") represents the first federal law protecting trade secrets. *See* H.R. Rep. 104–788, 1996 U.S.C.C.A.N. 4021, 4022–23. The EEA "creates a new crime of wrongfully copying or otherwise controlling trade secrets, if done with the intent either to (1) benefit a foreign government, instrumentality, or agent, or (2) disadvantage the rightful owner of the trade secret and for the purpose of benefitting another person." *Id.* at 4022.

There is no insinuation by either party that Shiah is a spy, or that the information possessed by Shiah affected national security. This case involves allegations that Shiah disadvantaged the rightful owner of the trade secrets, Broadcom, for the purpose of benefitting another person, Shiah and Marvell.

***14** Congress explained that "[f]or many years federal law has protected intellectual property through the patent and copyright laws. With this legislation, Congress will extend vital federal protection to another form of proprietary economic information-trade secrets." *Id.* at 4022–4023. The value of trade secret information "is almost entirely dependent on it being closely held." *Id.* at 4023. Congress further indicated that trade secrets information "includes, but is not limited to, information such as production processes, bid estimates, production schedules, computer software, and technology schematics." *Id.* at 4023. The need for such

legislation arose due to the increasing value of trade secrets to companies:

> For many companies this information is the keystone to their economic competitiveness. They spend many millions of dollars developing the information, take great pains and invest enormous resources to keep it secret, and expect to reap rewards from their investment. In the last few decades, intangible assets have become more and more important to the prosperity of companies.

Id. Furthermore, Congress noted the particular problems arising from computer technology:

> [i]ronically, the very conditions that make this proprietary information so much more valuable make it easier to steal. Computer technology enables rapid and surreptitious duplications of the information. Hundreds of pages of information can be loaded onto a small computer diskette, placed in a coat pocket, and taken from the legal owner.

Id. The pressing need for such a statute arose from the great value of trade secrets information and the conditions leading to their theft as described by Congress:

> This material is a prime target for theft precisely because it costs so much to develop independently, because it is so valuable, and because there are virtually no penalties for its theft. The information is pilfered by a variety of people and organizations for a variety of reasons. A great deal of the theft is committed by disgruntled individuals or employees who hope to harm their former companies or line their own pockets. In other instances, outsiders target a company, systematically infiltrate it, and then steal its vital information. More disturbingly, there is considerable evidence that foreign governments are using their espionage capabilities against American companies.

Id. Although Congress did intend to make it criminal for employees to use "knowledge about specific products or processes in order to duplicate them or develop similar goods for themselves or a new employer in order to compete with their prior employer," Congress struck a delicate balance between protecting information and allowing ideas to flow freely. *Id*. at 4026. Congress made it clear that the EEA was not "intended to be used to prosecute employees who change employers ... using general knowledge and skills developed while employed." *Id*. at 4026. America thrives on a competitive market, and California in particular provides for a competitive market as an at-will employment state. Congress did not intend to stifle creativity or prevent all information obtained in one job from being used in the next job. Given the congressional reasons for the enactment of the statute, there is some question about how compelling a case Congress would have viewed the current action against Shiah. Much of the alleged trade secret information in the Indictment Files is not information that Broadcom spent significant amounts of money developing independently – rather, it is pricing and marketing information. Shiah is not an outsider who targeted Broadcom or systematically infiltrated Broadcom. In addition, there is no indication that Shiah's goal was to harm Broadcom as a disgruntled employee or to line his own pockets. Although the Government argues that Shiah sought to line his own pockets by accepting an increased salary, the Government has also conceded that Marvell was not complicit in any of the alleged actions.

***15** Although the EEA is relatively new, this is not the first case that has proceeded to trial under the statute. *See, e.g., U.S. v. Lange,* 312 F.3d 263 (7th Cir.2002) (affirming Defendant's conviction for stealing computer data, including measurements and drawings of aircraft parts, from former employer and attempting to sell that data to former employer's competitor); *U.S. v. Yang,* 281 F.3d 534 (6th Cir.2002) (affirming Defendants' conviction for conspiring to steal the formula for acrylic adhesive developed by Avery);

United States v. Martin, 228 F.3d 1 (1st Cir.2000) (affirming Defendant's conviction for conspiring to steal trade secrets related to diagnostic test kits for pets and livestock).

D. The Elements

Each of the three counts refers to the nine Indictment files discussed above, all of which were downloaded from Shiah's Broadcom laptop to the Maxtor external hard drive on August 4, 2003. In order to find Shiah guilty for any of the three counts, all of the elements must be found with respect to at least one of these nine Indictment files.

1. Misappropriation, Unauthorized Duplication, and Possession of Computer Data Files Containing Information Related to Broadcom's Interstate and Foreign Business

The Government has proven, beyond a reasonable doubt, that Shiah misappropriated, duplicated without authorization, and possessed computer data files containing information related to Broadcom's interstate and foreign business.

The Maxtor external hard drive and CDs were found at Shiah's apartment on September 26, 2003 when the FBI searched the apartment. These computer media contained approximately 4,700 Broadcom files, including the nine Indictment files. Shiah purchased the Maxtor external hard drive in July of 2003, and he copied the files over to the Maxtor external hard drive during his last days as an employee of Broadcom, mostly on August 4, 2003. This has been established both by forensic analysis of the computer media, as well as Shiah's own admission. It is clear from the record that Shiah duplicated the files before leaving Broadcom, that he carried those files away from Broadcom's premises upon departure, and that those files were in his possession while he was working at Marvell, up until seized by the Government.

Furthermore, the record makes clear that Shiah's actions of copying these files and taking them with him when he left Broadcom were not authorized by Broadcom. The Confidentiality Agreement signed by Shiah indicated that Shiah was prohibited from taking confidential Broadcom documents after the termination of his employment, and Shiah has admitted that some of the information contained in the Indictment files constituted information that Broadcom would have considered confidential. Whitley indicated at the exit interview that Shiah should get rid of all Broadcom documents before leaving. In addition, the testimony of Broadcom employees indicated that Broadcom did not permit its employees to retain confidential documents after leaving the company. Thus, Broadcom did not authorize Shiah to copy, carry away, or possess after his departure from Broadcom the nine Indictment documents.

Finally, it is well established that information contained within the nine Indictment files relates to products which are sold outside of California and in foreign commerce. The documents contain information related to products sold to international PC manufacturers such as HP, Dell, and IBM. Thus, the data files contained information related to products Broadcom placed in interstate and foreign commerce.

***16** Accordingly, the Government has successfully met its burden of proving beyond a reasonable doubt that Shiah misappropriated, duplicated without authorization, and possessed without authorization the nine Indictment data files containing information relating to Broadcom's interstate and foreign business.

2. Computer Data Files Containing Information Constituting One or More Trade Secrets

The Government has also shown, beyond a reasonable doubt, that each of the nine Indictment files contains information constituting one or more trade secrets. As defined under the EEA, trade secrets include "all forms and types of financial, business, scientific, technical, economic or engineering information." 18 U.S.C. § 1839(3). The documents named in the Indictment in this action include information contained within those categories. Furthermore, in order for information to qualify as a trade secret, (1) the information must derive independent economic value from not being generally known to the public; and (2) the owner of the information must have "taken reasonable measures to keep such information secret." *Id.*

a. Information Deriving Independent Economic Value from Not Being Generally Known or Readily Ascertainable to the Public

The documents named in the Indictment contain a variety of information that is not generally known to the public, as evidenced by testimony of Young, Lakhani, Youngblood, Chang, and Ayer, in addition to Shiah's own testimony. At a minimum, the Indictment documents contain the following information that was confidential or not generally known to the public: (1) Indictment File # 1 (Std03Q3.xls)

contains internal costs, test and assembly yields, individual product revenue and margin information, and royalty information; (2) Indictment File # 2 (Palomar Concept Approval rev1.ppt) contains plans for the Palomar product, a product that had not yet been released on the market; (3) Indictment File # 3 (CA_arch1–0703.ppt) also contains plans for the Palomar product; (4) Indictment File # 4 (ROI_V008_PalomarDiablo_concept_approval.xls) also contains plans for the Palomar product; (5) Indictment File # 5 (Competitive GB Analysis 6–16–03.xls) contains information about the Palisades product, a product that Broadcom had not yet released to the market, as well as cost information for the 5705 product and detailed statistics on the number of gates used to perform various functions; (6) Indictment File # 6 (Tier 1 volumes.xls) contains customers' individual sales volume numbers and internal codenames for products sold by Broadcom's customers; (7) Indictment File # 7 (All Designs 7–24–03.xls) contains internal revision data and sales volume data for products sold by Broadcom, as well as internal codenames for products sold by Broadcom's customers; (8) Indictment File # 8 (Rebates 5–27–03.xls) contains Net ASP and rebate information pertaining to specific customers; and (9) Indictment File # 9 (Network cc action items 8–04–03.xls) contains notes pertaining to discussions about new products under development by HP, as well as other information known only between Broadcom and HP. Thus, each of the nine Indictment files contains some information that was not generally known to the public.

Furthermore, information contained in each of the nine Indictment files derived value from not being generally known to the public. For example, disclosure of the information contained in Indictment Files # 1 and 5 would allow competitors to compete more effectively with respect to price by undermining Broadcom's pricing structure and also obtain more favorable terms from their suppliers. Information pertaining to unreleased products, such as the information contained in Indictment Files # 2, 3, 4, and 5, would take away Broadcom's research and development advantage if it were disclosed to competitors. Furthermore, information pertaining to the number of gates used, as contained in Indictment File # 5, would give competitors the ability to try to match or beat Broadcom's performance by using less gates. Disclosure of customers' information in Indictment Files # 6, 7, and 9 would harm Broadcom's customer relations because of the customers' expectation that the information remain private. The internal revision and sales volume data contained in Indictment File # 7 could allow competitors to allocate their efforts toward certain products and compete more effectively. If customers knew other customers' Net ASP and rebate information, as contained in Indictment File # 8, then they would negotiate for higher rebates and lower Net ASP, reducing Broadcom's profits. Thus, the Government has shown, beyond a reasonable doubt, that each of the Indictment files contains some information that derived value from not being generally known or reasonably ascertainable.

***17** The Court notes, however, that much of the information contained in the files did not derive value from not being generally known to the public. Although the files contained confidential information, they also contained public information and information comprising general knowledge and skills obtained during Shiah's employment at Broadcom. This is information that Congress explicitly intended to exclude from the scope of the EEA. Therefore, it is important to avoid conflating access to these files with access to trade secret information. Nonetheless, each of these files contained some information that derived value from not being generally known to the public, which is sufficient to satisfy the first prong of the trade secret test beyond a reasonable doubt.

b. Reasonable Measures to Keep the Information Secret

The Government has also demonstrated, beyond a reasonable doubt, that Broadcom took reasonable measures to keep information contained within the nine Indictment files secret. Although there was much more that Broadcom could have done, the Court finds that the measures taken by Broadcom were barely sufficient to qualify as reasonable. However, the Court is also basing its determination on what would have been considered reasonable at the time, in 2003; the Court notes that the reasonableness standard will become more and more stringent as time passes. Over time, there will and have been improvements in technology, information, and knowledge pertaining to data secrecy, as well as more awareness of the EEA and its implications.

A trade secret is defined under the EEA to be information that is not generally known to the public. *See* 18 U.S.C. § 1839(3). Thus, the focus for this prong of the test should be whether Broadcom took reasonable measures to keep the information secret *from the public*. It is not required that the owner keep trade secrets from the trade secret holder's own employees; otherwise, “no one could do any work.” *Lange,* 312 F.3d at 266. The allegations in this case are that a Broadcom insider obtained confidential information while

employed at Broadcom, then took it with him to his next employer. It is not alleged that the information was leaked to members of the public. Nonetheless, it still could be the case that a company failed to take reasonable measures as a result of its failure to prevent an insider from departing with confidential information. After all, once an insider leaves with confidential information, the insider becomes an outsider and could potentially distribute the information to the public. This would lessen the secrecy of the information. The Court finds in this case, however, that Broadcom's measures, although not great, were still adequate to qualify as reasonable.

As explained above, Broadcom had a range of measures in place to keep information confidential. Broadcom's measures included a Confidentiality Agreement signed by every employee. The Confidentiality Agreement explained the value placed on confidentiality at Broadcom and attempted to indicate which documents were considered confidential. This document also prohibited employees from taking confidential information with them upon their departure. Furthermore, Broadcom protected its electronic data through its information technology team, which managed firewalls, file transfer protocols, intrusion detection software, passwords to access the Intranet, a layer of protection between the Intranet and Internet, and selective storage of files. When sharing information with outside entities, Broadcom required non-disclosure agreements, tracked the sharing through DocSafe, and marked documents as confidential. Finally, Broadcom maintained a high security physical facility.

Although Broadcom had numerous measures in place, there were deficiencies in the measures taken by Broadcom. There are a number of measures that Broadcom could have, and should have, taken in order to more effectively keep the information secret. At the beginning of his employment, Broadcom should have thoroughly explained the Confidentiality Agreement to Shiah before he signed it. Broadcom should have provided a copy of the Confidentiality Agreement to Shiah when he signed it, so Shiah would have it on record to refer to throughout his employment if he was not sure what to do in a specific situation. Broadcom should have trained Shiah about what information is confidential and how to handle confidential information. As explained by Naomi Fine (“Fine”), a defense expert, Broadcom should have provided education, training, or guidance to its employees regarding what information the company considered confidential. Fine also explained that the Confidentiality Agreement that Shiah signed was overbroad in that it designated almost all information confidential, making it hard to determine what information was actually confidential.

***18** Throughout Shiah's employment, Broadcom should have provided regular training as suggested by Fine. This training should have included methods for ensuring that information remained protected. Furthermore, Broadcom was not clear about which documents should and should not be marked confidential. Shiah was directed to use a template for all PowerPoint presentations containing markings to indicate confidentiality, but there were inconsistencies about which other documents were marked confidential. Broadcom did not have a comprehensive system in place for designating which documents were and which documents were not confidential. A better system could have made it easier for employees to determine which documents were confidential.

It is clear that Broadcom was simply trying to send a message to Shiah at his exit interview, rather than actually educate him. At the end of his employment, Broadcom should have specifically referred Shiah to the Confidentiality Agreement, showing him the copy he originally signed. Broadcom should have thoroughly explained the terms of the agreement again upon Shiah's departure. Broadcom should have ensured that Shiah read and signed Schedule C during his exit interview, keeping Schedule C on record to indicate that Shiah had read and signed it. Broadcom should have also asked whether Shiah had copied any files. Shiah explicitly asked questions about what information Broadcom considered to be a trade secret. He asked whether he could work with products in the same market while at another company. He asked whether it would be a problem if he worked with Broadcom's shared customers. What else should an exiting employee ask? Broadcom's answer that Shiah should consult an attorney did nothing to further Shiah's understanding of the terms of the Confidentiality Agreement he signed with Broadcom. Broadcom's goal should not have been to “scare” Shiah, but to inform him and give him guidance so that he would know what Broadcom permitted.

Broadcom sent an attorney to the exit interview, rather than Shiah's supervisor who was innately familiar with Shiah's work. Shiah's supervisor could have provided details about which information was particularly sensitive. The attorney was only able to make broad and general claims. The only choice that Broadcom presented Shiah was that he could not take anything with him upon departure. Clearly, it is within Broadcom's interest to make the restrictions as broad as possible. However, such an approach has a severe chilling

effect on employees' abilities to change jobs and take general skills and knowledge with them upon doing so. Congress never intended to restrict employees' abilities to take general skills and knowledge with them. Broadcom wanted to send a message to Shiah in his exit interview, just as Broadcom wants to send a message to future employees through this criminal prosecution. However, criminal prosecution is not the forum for such a message.

Finally, Broadcom could have further protected itself by checking Shiah's computer upon his departure, particularly where Broadcom suspected that Shiah was going to Marvell and Broadcom worried about the confidential information that Shiah might take with him. If someone from Broadcom had taken the simple step of looking at the data on Shiah's computer, he or she would have been able to easily observe the access dates on the files to determine that Shiah had recently copied thousands of files from the computer. Broadcom would have been able to confront Shiah about it immediately. This would have been a more effective approach than investigating Shiah's actions after the fact and ultimately submitting a document to the Government to recommend criminal prosecution. Rather than preventing the conduct up front, Broadcom addressed it on the back end. Broadcom's most pressing interest would presumably be to protect the information, which it claims to be of such great value. Yet, Broadcom knowingly watched Shiah leave to take a job with its competitor Marvell in a highly competitive industry without taking the steps mentioned above to prevent him from taking trade secrets with him. In effect, although not responsible for Shiah's actions, Broadcom's inaction contributed to Shiah being in such a position.

***19** Furthermore, Broadcom's failure to take these steps has deprived the Court, as the trier of fact, of evidence that might have placed the prosecution on more solid footing with respect to Shiah's intent. For instance, if Broadcom had explicitly asked Shiah about whether or not he was taking information with him, or required Shiah to sign Schedule C and spoken to Shiah about the repercussions of Schedule C, then Shiah's actions in response may have provided valuable evidence about Shiah's alleged intent to convert trade secret information. In addition, if Broadcom had inspected Shiah's computer before he departed and confronted him about copying thousands of files, Shiah's response would have been highly probative of his intent. If Shiah had lied about the files, then the Government would have very strong evidence to establish Shiah's intent beyond a reasonable doubt – a standard the current evidence fails to satisfy, as discussed below. If Shiah's supervisor had been present at his exit interview, he could have asked Shiah specific questions about specific documents; if Shiah had lied, this Court would have all the evidence it needs to convict Shiah. Instead, Broadcom waited around while misconduct took place, conducted its own investigation, and then solicited the Government to prosecute based on that misconduct after the fact, depriving the Court of potential evidence and failing to prevent confidential information from leaving its premises.

Nonetheless, the Court finds that the deficiencies in Broadcom's measures were not so extensive to qualify as unreasonable; Broadcom barely satisfies the standard of reasonableness. As a whole, the measures taken by Broadcom were generally effective. The Broadcom employees' testimony indicated that they generally understood what types of information were considered confidential. When asked about particular documents, Lakhani, Youngblood, and Shiah, the three PLMs, were able to indicate which information they believed Broadcom considered confidential in 2003. The testimony of Broadcom employees throughout trial also indicated that Broadcom's culture was one in which confidentiality was valued and protected. Furthermore, Venner explained that Broadcom was known for having a stingy reputation with regard to data protection. The measures that Broadcom did have in place indicate that Broadcom had thought about its data security and had built mechanisms in an attempt to protect its vital information. Thus, in general, Broadcom had reasonable measures in place to keep its information secret. The Government has met its burden of showing, beyond a reasonable doubt, that Broadcom took reasonable measures to keep its information secret.

Accordingly, the Government has proven, beyond a reasonable doubt, that the nine Indictment files each contain information constituting one or more trade secrets. However, the Court notes that much of the value of the information was time-sensitive, in that it was less likely to qualify as trade secret information with the passing of time. For instance, the pricing and product information was bound to change over time as new contracts and products were developed. Much of this information became irrelevant in a short period of time after Shiah left Broadcom. In this regard, although the files contained trade secret information, this information was not Broadcom's crown jewels, as the Government would have the Court believe.

In addition, while one reason for Broadcom to keep information in the Indictment Files confidential was because

it derived economic value from being private, another motive driving Broadcom was likely the embarrassment that would result if its clients were made aware of the significant price differences between clients exemplified in files such as Rebates 5–27–03.xls. Furthermore, Broadcom sought to bring as much information as it could within the scope of its trade secrets in order to stifle competition and lessen the exchange of employees and information to its competitors. However, it was Broadcom that chose to operate its business in California, an at-will employment state. In order to obtain the benefits of operating its business in California, such as creativity and a free-flowing employment marketplace, Broadcom must also be prepared to accept the aspects of this market that may be less beneficial to it. If the Court were to uphold such broad definitions and restrict information as desired by Broadcom, the effect would severely chill competition. Thus, the Court strictly limits its definition of trade secret information to that information which very clearly meets the definition set forth in the EEA.

3. Knowledge that the Computer Data Files Contained Information Constituting One or More Trade Secrets

***20** The Government has also satisfied its burden of proving, beyond a reasonable doubt, that Shiah had knowledge that each of the nine Indictment files contains information constituting one or more trade secrets. With the exception of Indictment File # 9 (Network cc action items 8–04–03.xls), Shiah expressly indicated his knowledge of portions of information in each of the Indictment files that Broadcom would have considered to be confidential in 2003. Furthermore, Indictment File # 9 (Network cc action items 8–04–03.xls), as well as Indictment File # 1 (Std03Q3.xls), Indictment File # 2 (Palomar Concept Approval rev1.ppt), Indictment File # 3 (CA_arch1–0703.ppt), and Indictment File # 4 (ROI_V008_PalomarDiablo_conceptVapproval.xls) were all marked to indicate that they were confidential documents.

In addition, there is ample circumstantial evidence indicating Shiah's knowledge that the documents contained confidential information, or information not generally known to the public. For one, Shiah signed the Confidentiality Agreement at the beginning of his employment with Broadcom, making him aware of the importance of confidential information at Broadcom. In addition, Whitley discussed the importance of protecting Broadcom's confidential information at Shiah's exit interview and indicated that this information included technical documents, business information, and road maps. Furthermore, the testimony of Shiah's co-PLMs and other coworkers indicated that they had knowledge of which information was publicly available and which information would lose value if it was publicly known. Although Shiah testified based on his own sense of what information was confidential, as did the other employees, the consistency between their testimony indicates that they were able to determine, with reasonable accuracy, which information was sensitive.

Finally, even though Broadcom did not distinguish between proprietary information and trade secret information, Shiah's knowledge that information constituted a trade secret in the context of the EEA can be inferred, even if Shiah was not familiar with the term, “trade secret.” Specifically, Shiah's role as a PLM, knowledge of marketing, and his familiarity with the value of the information in the Indictment files leads to an inference that he knew that some of the confidential information in the Indictment files derived economic value from not being generally known, thus meeting the definition of a trade secret under the EEA. This holds true even though Whitley told Shiah to consult an attorney when Shiah asked what information constituted trade secret information. Broadcom was not required to identify certain information as being confidential and identify certain other information as being trade secret information in order for information to qualify as a trade secret under the EEA.

Thus, Shiah's stated knowledge, as well as the circumstantial evidence, indicate that the Government met its burden of showing that Shiah knew that the each of the nine computer data files named in the Indictment contained information constituting one or more trade secrets.

4. Intent to Convert One or More of the Trade Secrets to the Economic Benefit of Anyone Other than Owner with Intent or Knowledge that Owner Would be Injured

Finally, in order for the Court to find Shiah guilty of any of the three counts in the Indictment, the Government would have to demonstrate, beyond a reasonable doubt, that Shiah intended to convert one or more of the trade secrets in one of the nine Indictment files to the economic benefit of anyone other than Broadcom, with the intent or knowledge that Broadcom would be injured. The Government falls just short of its burden of showing, beyond a reasonable doubt, that Shiah intended to convert one or more of the trade secrets in one of the nine Indictment files. Here, Shiah's intent may not be proven directly because there is no way of directly scrutinizing the workings of the human mind. Thus, the Court

looks to the circumstances surrounding Shiah's actions to determine Shiah's intent and finds that the requisite intent has not been shown beyond a reasonable doubt.

***21** Here, Shiah's explanation, which is sufficient to create a reasonable doubt with respect to the nine Indictment files, is that he copied all of the approximately 4,700 files in order to have a complete repository of all files and information related to his job at Broadcom. This was Shiah's "toolkit," and his actions were in line with his past actions from prior jobs and experiences. He claims that he did not intend to use any of the information that Broadcom would have considered confidential in any of the files he accessed. The fact that the documents contained trade secret information, as well as non-confidential information, creates reasonable doubt about which information Shiah accessed when he viewed the files. The Court cannot expect an employee to know the contents of every document prior to accessing it in order to avoid opening those documents that contain some trade secret information for the purposes of preventing liability under the EEA. In order to find liability, there must be a showing that the file was accessed with the intent of converting trade secret information. Without a strong showing that Shiah intended to use the trade secret information in the documents, the Court cannot find Shiah guilty.

Shiah relied on his own internal filter to determine what information was confidential and what information he could access and use after departing from Broadcom. While employed at Broadcom, he was also required to rely on his own discretion to determine which information was confidential and which information could be revealed. Furthermore, he was required to do the same with respect the information he remembered after leaving Broadcom. Given the short time period between Shiah's job at Broadcom and Shiah's job at Marvell, Shiah also retained in his memory much of the information that he learned while working at Broadcom. Shiah was similarly required to make judgment calls about the information in his memory based on his assessment of whether that information was confidential to Broadcom or not. In other words, Shiah possessed trade secret information both in the files that he copied and in his memory. Shiah claims that, for both categories of information, he relied on his understanding of what information was confidential in order to only use that information that would not be considered confidential or a trade secret.

The nine Indictment files form the basis of the relevant counts, and the Court must examine whether Shiah intended to convert any of the trade secret information in any of the nine Indictment files. Of the nine files listed in the Indictment, Shiah only accessed five after leaving Broadcom. Those five files are: (1) Indictment File # 5 (Competitive GB Analysis 6–16–03.xls); (2) Indictment File # 6 (Tier 1 volumes.xls); (3) Indictment File # 7 (All Designs 7–24–03.xls); (4) Indictment File # 8 (Rebates 5–27–03.xls); and (5) Indictment File # 9 (Network cc action items 8–04–03.xls). Shiah created Indictment Files # 5–8 while working at Broadcom. He did not create Indictment File # 9, but instead received it by email the afternoon of August 4, 2003. Shiah did not access Indictment Files # 1–4 at any time after downloading them on August 4 to the external hard drive.

The Court finds that the Government has failed to show the requisite intent with respect to Indictment Files # 1–4. Shiah never accessed these files after copying them to the Maxtor external hard drive. Furthermore, all of the files were included in the general download of approximately 4,700 files from Shiah's Ethernet folder on his Broadcom laptop to the Maxtor external hard drive. Finally, Shiah has reasonable explanations for the means by which he originally obtained each of these documents. Indictment File # 1 (Std03Q3.xls) was sent to Shiah via email by Chang after an email dialogue through which Shiah attempted to clarify pricing on several Broadcom products. Shiah received Indictment File # 2 (Palomar Concept Approval rev1.ppt) in an individual email from Lakhani and received it a second time in an email sent by Lakhani to a group of Broadcom employees including Shiah. Elzer, the marketing manager for the ethernet group, sent Indictment File # 3 (CA_arch1–0703.ppt) to Shiah in a group email sent to numerous Broadcom employees. Finally, Shiah requested Indictment File # 4 (ROI_V008_PalomarDiablo_concept_approval.xls) from Lakhani in order to understand the background calculations and received it immediately in an email from Lakhani. He had also previously obtained the same file.

***22** A finding that the Government has proven, beyond a reasonable doubt, that Shiah intended to convert the trade secret information in Indictment Files # 1–4 would be the same as a finding that Shiah intended to convert the trade secret information of all 4,700 files that were included in Shiah's general transfer of documents. The Government has not shown Shiah's intent to convert these files beyond a reasonable doubt, where the files were included in a general transfer, were never accessed after the general transfer, and were obtained through reasonable means that appear to be in the normal course of Shiah's employment at Broadcom.

This is particularly true in light of Shiah's explanation that he intended to copy all files and documents related to his work at Broadcom, intending to later use only that information which was not considered to be confidential.

Of the remaining five Indictment files, all of which Shiah did access during his employment at Marvell, Shiah accessed two of these files on September 8, 2003, and he accessed three of these files on September 16, 2003. On September 8, Shiah accessed Indictment File # 5 (Competitive GB Analysis 6–16–03.xls) and Indictment File # 6 (Tier 1 volumes.xls). Both of these files were created by Shiah while he was employed by Broadcom. Thus, there is nothing suspicious about the way in which he originally obtained these files. They were also both part of the general transfer of approximately 4,700 files on August 4, 2003. Again, the Court finds Shiah's explanation for the reasons behind his general transfer of documents to be reasonable. Although it was not permitted by Broadcom and would likely subject Shiah to civil liability, it did not, alone, amount to a violation of the EEA. Accordingly, Shiah's access of these files is the most pertinent evidence from which to determine Shiah's intent with respect to the trade secret information contained within the files.

The evidence surrounding Shiah's access on September 8 does not establish, beyond a reasonable doubt, that Shiah intended to convert any of the trade secret information contained within Indictment Files # 5 and 6. While accessing the Maxtor external hard drive on September 8, Shiah created a new document entitled Competitive GB analysis.xls. Competitive GB analysis.xls contains no trade secret information. Furthermore, the first page of Competitive GB analysis.xls is nearly identical to the first page of Indictment File # 5. Thus, this evidence indicates that Shiah accessed Indictment File # 5 in order to copy the first page into the new document. None of the information copied was trade secret information. The Government has sought to prove that Shiah accessed Indictment File # 5 in order to access the cost information for the Broadcom 5705 product and set lower prices for competing Marvell products in an RFQ that was submitted to IBM that same day. Shiah denies that he was involved in setting the prices for the IBM RFQ; the burden rests with the Government. In light of Shiah's clear purpose of accessing Indictment File # 5 to copy non trade secret information, and in the absence of more evidence supporting the Government's suspicions with respect to price setting, the Court finds that the Government has not shown, beyond a reasonable doubt, that Shiah intended to convert trade secret information in Indictment File # 5.

Shiah claims that he accessed Indictment File # 6 in order to view aggregate PC volume information. He wanted to understand overall market size as part of his role of marketing director. The aggregate sales volume information was publicly available and is not trade secret information. Shiah's explanation for this file is consistent with an explanation that he used his discretion to determine which information could be accessed and used. Without contrary evidence, the Government has not shown, beyond a reasonable doubt, that Shiah intended to convert any of the trade secret information contained in Indictment File # 6.

***23** Shiah accessed the remaining three Indictment files, Indictment File # 7 (All Designs 7–24–03.xls), Indictment File # 8 (Rebates 5–27–03.xls), and Indictment File # 9 (Network cc action items 8–04–03.xls), on September 16, 2003. Shiah created Indictment Files # 7 and 8 while employed at Broadcom. He received Indictment File # 9 in an email sent on August 4, 2003, whose recipients included Shiah as well as other Broadcom employees. With respect to these files, there is nothing suspicious about the way they were originally obtained by Shiah. Furthermore, Indictment Files # 7 and 8 were included in the general transfer of approximately 4,700 files to the Maxtor external hard drive on August 4, 2003. Shiah added Indictment File # 9 to the Maxtor external hard drive the same day, after receiving it by email. Shiah's explanation is that he wanted to included all files in his "toolkit." The Court finds that his selective copying of this specific document is consistent with Shiah's explanation for the general transfer of documents; he intended that the "toolkit" be comprehensive. Again, the Court turns to the evidence surrounding Shiah's access of these files on September 16, as it did with the files accessed on September 8.

The evidence surrounding Shiah's access on September 16 does not establish, beyond a reasonable doubt, that Shiah intended to convert any of the trade secret information contained in Indictment Files # 7–9. Shiah claims that he accessed these files to find other sources of aggregate volume information for PC manufacturers in order to cross-check the information he had already obtained from Indictment File # 6. This aggregate volume information does not fall within the definition of a trade secret. Shiah's access occurred two days before Shiah gave a presentation that contained information about market size, market share, and aggregate volume regarding PC companies, including companies that were not referenced in Indictment File # 6. None of the information contained in the presentation Shiah gave on September 18 is

information that would have been considered confidential to Broadcom. Indictment File # 7 contained aggregate volume information, although not the type that Shiah claims he was seeking. Shiah explains that he thought Indictment File # 9 might have the information he was seeking, but found out that it did not after opening it. Finally, Shiah claims that he thought Indictment File # 8 would contain total rebate calculations from which he could derive aggregate volume information. However, he found out that it did not contain total rebate calculations. As oftentimes occurs when users attempt to find a file or information, Shiah explains that he opened several files thinking they might contain the information he was seeking, only to find out that they did not.

The Government seeks to prove that Shiah accessed these files in response to action items regarding Marvell's business with HP. Indictment File # 7 contains information regarding HP's programs, but it also contains information about many other PC manufacturers. Indictment File # 8 contains pricing information for HP, but, again, also contains information about many other PC manufacturers. Finally, Indictment File # 9 contains notes of Broadcom calls with HP regarding product issues, as do several other files that Shiah accessed on the same day. Shiah responded to an HP action item regarding power demands of the Yukon product on September 16. However, the Government has not shown, beyond a reasonable doubt, a link between Shiah's response to the action item and the use of trade secret information in that response obtained from the files Shiah accessed on September 16. Specifically, there is no showing of particular trade secret information contained within any of these files that Shiah converted for his use at Marvell; nothing links Shiah's access with nefarious use or any other use of trade secret information. While the pattern of access is suspicious, the allegations of intent based on this pattern are too speculative to demonstrate Shiah's intent to convert trade secrets in Indictment Files # 7–9 beyond a reasonable doubt. While the Court finds that the evidence makes it more likely than not that Shiah intended to convert trade secrets in these files, satisfying a preponderance standard, Shiah's explanation for his actions are sufficient to create a reasonable doubt.

***24** The Government also argues that the circumstances surrounding Shiah's overall attempts to obtain files prior to leaving Broadcom indicate his intent to convert trade secrets in the Indictment files for his benefit. Shiah's efforts to gather files are consistent with an explanation that he was trying to gather as many trade secrets as possible before leaving Broadcom. However, his efforts are also consistent with an explanation that he was trying to make sure he included all potential information that might have related to his work at Broadcom in his "toolkit," so that he would ultimately be able to use his discretion to determine which of the non-confidential information to use in the future. In addition, there are other potential explanations to support Shiah's acquisition of documents. For one, Shiah had just received a negative performance review, indicating that he needed to better understand the developing technologies, follow up more with customers, and be more aggressive in marketing products. It is reasonable that Shiah sought some of these files in order to increase his understanding of the products and the market. He also may have been trying to improve his performance by working diligently to the end of his job at Broadcom and seeking to leave a good impression upon his departure. Even though he knew he was going to leave, he was still involved in substantive work. For instance, Shiah sent an email concerning matters related to Fujitsu and the 4401B product on his second to last day on the job. These potential explanations cast reasonable doubt on a theory that Shiah was trying to acquire all of this information for the purposes of gathering trade secret information with the intent to convert that information.

Finally, the Government argues that intent can be inferred from the overall circumstances, not just those pertaining to the Indictment files, surrounding Shiah's data access on the Maxtor external hard drive while employed at Marvell. In doing so, the Government seeks to demonstrate Shiah's intent with respect to other files in order to create an inference of intent with respect to the Indictment files. However, the Court must also look to the circumstances surrounding those Indictment files. As discussed above, the Court has found that reasonable doubt exists in the circumstances surrounding Shiah's access of the Indictment files. Furthermore, Shiah has set forth an explanation for each file he accessed that, if true, would demonstrate a lack of intent to access the files for the purpose of converting trade secret information. Even if the circumstances surrounding some of Shiah's access to other non Indictment files are suspicious, the Court finds that they do not negate the reasonable doubt that exists regarding Shiah's intent to convert trade secret information contained in the Indictment files.

There are a number of circumstances that do not exist in this case that, if shown, would be more likely to demonstrate intent to convert trade secrets beyond a reasonable doubt. There is no evidence that Shiah, an engineer, took steps to clear evidence from his Broadcom laptop that he accessed

thousands of files at the same time on August 4, 2003. In addition, there is no evidence that Shiah distributed trade secret information while working at Marvell. For example, the evidence pertaining to Shiah's access of the Dell related files on September 22, 2003 demonstrates that the only information Shiah shared with O'Connor after accessing those files was the requested contact information, despite the fact that those files contained much more information, including confidential information. This demonstrates Shiah's limited intent in accessing the files, as well as his limited distribution of information to other employees of Marvell.

Finally, there is no evidence demonstrating trade secret information taken from files obtained by Shiah while working at Broadcom and used directly in documents or other work product produced by Shiah while working at Marvell. It is perhaps most noteworthy that Shiah had ample opportunity to use trade secret information from the Indictment files during his time employed at Marvell. Yet, despite this opportunity, there is no clear evidence demonstrating trade secret information that was converted into any of Shiah's work product. The most suspicious access occurred on September 16, 2003. That access does not demonstrate beyond a reasonable doubt that Shiah actually took trade secret information from the files he accessed, and then used that information in files or other work product he produced. There is no clear evidence showing trade secret information that Shiah used in his response to the HP action items, and the presentation Shiah gave on September 18 does not include any confidential information. Furthermore, prior to this access, there were many projects and opportunities which would have created tempting circumstances for Shiah to use trade secret information in his work product. This would be particularly true if Shiah intended to take advantage of the trade secret information contained within the files. However, direct evidence to show that he actually used trade secret information is not clearly established on the record. The Court would expect a guilty person to take absolute advantage of trade secret information and actually use the information wherever the opportunity to do so arose. If Shiah were guilty, the Court would expect him to give presentations and produce documents containing trade secret information. He would likely go out of his way to offer information to other people at Marvell and take credit for that information. He would have gone outside of his departmental expertise to offer trade secret information for specific Broadcom engineering designs or other information if he were guilty. However, Shiah did not take such action, and if he did, the Government failed to prove that he did. Such additional evidence, if it existed, would erase the reasonable doubt. In light of the evidence that is missing from the record and the reasonable doubt that exists, the Court concludes that the Government has failed to show Shiah's intent to convert trade secrets in the Indictment files beyond a reasonable doubt.

***25** If the Government had gathered more evidence and conducted surveillance before searching Shiah's apartment, the likelihood of obtaining additional probative evidence would have increased. However, much of the evidence supporting the search of Shiah's residence was evidence obtained from Broadcom's investigation and provided by Broadcom to the Government, rather than evidence directly obtained by an investigation conducted by the Government. There are dangers that result from private companies conducting their own investigations, then subsequently presenting the evidence to the Government. First, private companies do not have the same level of expertise that Government agents have acquired through years of training and practice. Accordingly, there may be holes in the evidence, as can be seen by certain evidence that is missing in this case. Furthermore, when the FBI adopts evidence provided by private entities, it does not gain the same level of understanding and knowledge of the evidence that it would have obtained if it had conducted the investigation itself. When the investigation is driven by a private entity, the process is deprived of the same level of prosecutorial judgment and discretion that accompanies a typical Government investigation conducted from scratch. In a highly competitive market, there is strong incentive for a private entity to present evidence to the Government in the light most favorable to that entity, rather than viewing the evidence objectively. The private entity may place significant pressure on the Government to pursue criminal prosecution. If such an approach is condoned, then criminal investigations may fall substantially in the hands of civil organizations, and the prosecutorial role may become tainted.

When incarceration is at stake, the investigation should be conducted by law enforcement, not law enforcement and a private corporation together. The hybrid nature of the investigation has appeared to have other effects on the progress of the action. Broadcom began its involvement in this case nearly three years before the Indictment was filed, urging criminal prosecution and gathering evidence to support the case. The Court is concerned about the significant delay and clear lack of diligence on the Government's part in filing this case. Such a delay leaves the trier of facts in a quandary as to why it took so long to proceed.

In closing, the Court notes that there is no question that Shiah's actions were wrong and that they were not permitted by Broadcom. Furthermore, Shiah's actions would very likely subject him to civil liability. The Court simply finds that the evidence does not show, beyond a reasonable doubt, that Shiah's actions subject him to criminal liability under the EEA. When life and liberty are involved, proof beyond a reasonable doubt is mandated. Reasonable doubt has a bite, and it is a heavy burden falling on the Government that distinguishes civil actions from criminal actions. In light of all the circumstances surrounding this action, reasonable doubt exists about Shiah's intent to require a finding of not guilty. A contrary holding would not only deprive Shiah of his liberty without holding the Government to its high burden, but it would also have a chilling effect on the ability of employees to move freely from one company to another. If the Court found Shiah guilty without more evidence to support his intent, employees might avoid movement between companies due to the risk of prosecution arising from information carried with them, either in their minds or in physical form. Such a result would be contrary to Congress' intent that the EEA not "be used to prosecute employees who change employers... using general knowledge and skills developed while employed." See H.R. Rep. 104-788, 1996 U.S.C.C.A.N. 4021, 4026. If the Court was to find Shiah guilty on the basis of the evidence presented, then the Court could present a significant number of cases on its civil calendar that are much more susceptible and worthy of prosecution as a criminal matter. The Government has not shown, satisfactory to its high level of proof of beyond a reasonable doubt, that Shiah intended to do more than using general knowledge, skills, and information obtained at Broadcom while employed at Marvell.

DISPOSITION

For the above mentioned reasons, the Court finds Tien Shiah NOT GUILTY of the following three counts in the Indictment:

(1) Stealing and Misappropriating Trade Secrets under 18 U.S.C. § 1832(a)(1);

(2) Copying and Duplicating Trade Secrets under 18 U.S.C. § 1832(a)(2); and

(3) Possessing Stolen or Misappropriated Trade Secrets under 18 U.S.C. § 1832(a)(3).

IT IS SO ORDERED.

All Citations

Not Reported in Fed. Supp., 2008 WL 11230384