No. 14-10037; 14-10275

IN THE UNITED STATES COURT OF APPEALS

FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

v.

DAVID NOSAL,

Defendant-Appellant.

Appeal from the United States District Court
for the Northern District of California
District Court No. CR 08-0237 EMC

APPELLANT'S OPENING BRIEF

DENNIS P. RIORDAN (SBN 69320)
dennis@riordan-horgan.com
DONALD M. HORGAN (SBN 121547)
don@riordan-horgan.com
RIORDAN & HORGAN
523 Octavia Street
San Francisco, CA 94102
Telephone: (415) 431-3472
Facsimile: (415) 552-2703

TED SAMPSELL-JONES
William Mitchell College of Law
875 Summit Avenue
St. Paul, MN 55105
Telephone: (651) 290-6348

Attorneys for Defendant-Appellant
DAVID NOSAL

TABLE OF CONTENTS

Table of Contents continued

Table of Contents continued

Table of Contents continued

TABLE OF AUTHORITIES

CASES

Table of Authorities continued

Table of Authorities continued

Table of Authorities continued

Table of Authorities continued

Table of Authorities continued

STATUTES

OTHER AUTHORITIES

INTRODUCTION AND SUMMARY OF ARGUMENT

This case has already produced one en banc opinion. *United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012). After a remand and trial, this case now returns with an appeal raising fundamental questions about the scope of two important federal statutes: 18 U.S.C. § 1030, the Computer Fraud and Abuse Act (CFAA); and 18 U.S.C. § 1832, the Economic Espionage Act (EEA). These statutes were intended to combat grave threats to legitimate modern commerce–computer hacking and theft of trade secrets. This Court must decide whether the criminal provisions of the CFAA and EEA should be stretched to reach wrongful but relatively common employee misconduct.

In this case, employees and former employees of Korn Ferry International (KFI), an executive search firm, downloaded "source lists" from KFI's computers. The source lists consisted of names, positions, and contact information for executives who were potential candidates for placement in searches that KFI had conducted or was conducting at the time of the downloads. The downloads were to be used by the defendant, David Nosal, who had left KFI to start his own executive search firm, and were conducted by Mr. Nosal's alleged co-conspirators, who were planning to join him in his new venture.

Most breaches of a company's code of conduct are not federal crimes. Most acts of employee misappropriation are appropriately addressed by private civil remedies and state criminal law. In fact, KFI filed civil claims against its former employees. The government nonetheless sought to pursue this case under a

variety of federal criminal statutes. Many of its theories have already been rejected. The government initially charged Mr. Nosal with multiple counts of mail fraud, but those charges were dismissed prior to trial. The district court also dismissed most of the CFAA charges. Rejecting the government's interlocutory appeal, this Court affirmed that dismissal because the downloads did not involve hacking, and thus did not violate the CFAA. *Nosal*, 676 F.3d 854.

After the appeal, the case returned for trial on the remaining counts, which this Court has not yet reviewed. Mr. Nosal was convicted on these counts, but the legal theories underlying the convictions are flawed. The remaining CFAA counts do not constitute a criminal offense under this Court's opinion in *Nosal*: the downloads in question were effectuated by the consensual use of a password validly issued to a KFI employee, and thus involved no hacking. The district court's jury instructions on the CFAA charges also included multiple errors.

The convictions for theft of trade secrets are also flawed, because the source lists taken from KFI do not meet the legal definition of "trade secrets." Trade secrets must be *secret*, and the "secrets" at issue here consisted of information readily ascertainable in the public realm. The government relied on an argument that the source lists were proprietary "compilations," but Congress never intended every wrongful taking of a private compilation of public information to be a violation of the EEA. Moreover, the sine qua non of a trade secret under federal law is the requirement that its holder vigorously protect its content from public disclosure. The evidence at trial showed that KFI commonly sold and distributed

its sources lists. Mr. Nosal is entitled to acquittal on the trade secret counts as well; at a minimum, the jury instructions defining these offenses were also flawed.

Finally, the district court permitted the government to introduce highly prejudicial evidence that concededly was irrelevant to Mr. Nosal's guilt or innocence, while barring the defense the opportunity to rebut that evidence.

This case should not have produced federal criminal charges. KFI marshaled its massive resources to convince federal prosecutors to obtain an indictment that would justify the denial to Mr. Nosal of over a million dollars in compensation the company owed to him. In its lobbying of the government to indict Nosal, KFI claimed that the downloaded source lists were worth twelve million of dollars, but the district court put the value of the information at a small fraction of one percent of that amount. Employee misconduct does not rise to the level of a serious federal felony simply because a major corporation wants it to be so. Mr. Nosal's convictions must be reversed.

STATEMENT OF JURISDICTION

The district court had jurisdiction under 18 U.S.C. § 3231. This Court has jurisdiction under 28 U.S.C. § 1291. This appeal is from an amended final judgment of conviction, entered by the district court on May 30, 2104. (ER169.) The notice of appeal was filed on June 5, 2014. (ER 167.)

BAIL STATUS

Mr. Nosal is not in custody. He was sentenced to imprisonment, but the district court stayed the sentence pending the outcome of this appeal.

STATEMENT OF THE CASE

The government indicted Mr. Nosal in April of 2008, and it filed a superseding indictment in June of 2008. The superseding indictment contained twenty counts. Most of the counts were dismissed prior to trial. The government unsuccessfully appealed the dismissal of certain counts, and the case returned to district court for trial.

The government filed a second superseding indictment, containing six counts, in February 2013. (ER 1164-78.) It alleged three substantive violations of the CFAA, 18 U.S.C. § 1030. It alleged two substantive violations of the EEA, 18 U.S.C. § 1832. It also alleged one count of conspiracy to violate the CFAA and EEA.

Jury trial commenced before the Honorable Edward Chen on April 9, 2013. The jury returned its verdict on April 24, 2013, finding Mr. Nosal guilty of all six counts. Judge Chen imposed judgment and sentence on January 8, 2014. (ER 178.) Mr. Nosal filed a timely notice of appeal. (ER 176.) On May 30, 2014, Judge Chen filed an amended judgment containing a restitution order. (ER 169.) Mr. Nosal again filed a timely notice of appeal. (ER 167.)

STATEMENT OF FACTS

A. Korn Ferry and its Searcher Database

Korn Ferry International (KFI) is the world's largest executive search firm. It is a publicly traded company with annual revenues approaching $1 billion. Headquartered in Los Angeles, it has several thousand employees in offices

around the world. Most of KFI's revenues come from executive recruitment: KFI is typically hired by other businesses in order to identify and recruit executives. KFI also sells other business consulting services.

KFI often generates its executive search revenue by making "pitches" to other companies. (ER 849.) KFI employees work in teams to win business. A team will generally bring a list of potential executive candidates to a potential client as part of the pitch. (ER 850.) These candidate lists, which often have been used in prior executive searches conducted by KFI, are referred to as "source lists." (ER 855; Tr.234:7-9.) The team will present those names in order to demonstrate its expertise and its ability to successfully complete the search and placement process. (ER 675-76.) If the KFI team wins the client's business, then it prepares a position specification that defines in greater detail exactly what type of position the client is seeking to fill. (ER 851.) KFI then prepares a more refined and more detailed list of potential candidates to present to the client to be further winnowed before candidate interviews are conducted. (ER 858, 885.)

KFI derives its source lists from Searcher, its own internal database of executives and potential candidates. (ER 712.) Searcher is a database containing names, contact information, job history, salaries, and other notes for many individual executives. The Searcher database is compiled from a variety of different sources. Much of the information comes from public sources, such as LinkedIn, Hoover, filings by public corporations, newspapers, or simply by googling an individual's name. (ER 413-18, 475, 582, 881.) KFI received

"hundreds and hundreds" of unsolicited resumes each week from executives who wished to be considered as candidates for searches. (ER 585) Additionally, thousands of candidates input their information directly into Searcher, via KFI's website. (*Id*.)

Other information is derived from KFI employees' personal knowledge. KFI employees are encouraged by the firm to add to the database. KFI employees input information that they know from personal connections and prior employment, including information they bring from prior search firms. (ER 578-79, 614, 795-96, 869-71, 874-75.) It was common in the industry for people, including people at competing firms, to share information. (Tr.1196-98.) It was also a common industry practice for recruiters to bring with them contact and executive information that they had developed at a prior search firm. (ER 423.) A person's name and phone number entered into Searcher would not be considered KFI's confidential or proprietary information (ER 1011-12), nor would information in Searcher that came from an employee's personal knowledge or personal data (ER 1008-09).

In short, there is an enormous amount of public and non-proprietary information in Searcher. (ER 585, 598-99.) Moreover, once a name is put into Searcher, there is no way to know where information on a source list originated. (ER 610-13, 877-78, 882.)

The Searcher database resides on KFI's computer system. On that same computer system KFI maintains similar information products like Hoovers,

OneSource, Factiva, Nexus. (ER 690.) KFI employees and independent contractors have access to the database. It is mostly used by lower and mid-level employees rather than by partners. A password is required to access KFI's computer system, but once in the system, no separate password is required to access the Searcher database. KFI has a policy that prohibits employees from sharing passwords or KFI accounts (ER 701-03), but KFI employees routinely shared passwords (ER 426). Searcher is an "open" database, meaning that all of the information in Searcher is available to anyone who has access to it.

Source lists are disclosed to clients during pitches (ER 424), and sold to clients as part of "road map" or "mapping" engagements (ER 590). KFI employees regularly emailed source lists around, or took them home. (ER 421-22.) Source lists were emailed to people outside of KFI; there was nothing to prevent the lists from being distributed outside KFI. (ER 422, 428-29, 447.)

B. Nosal's Employment and Departure from KFI

Mr. Nosal was employed at KFI from 1996 to 2004. He was a high-ranking executive and a top revenue producer. At the time of his departure, Mr. Nosal was the Managing Director of KFI's Silicon Valley office. He was also regional Managing Director. But by early 2004, the relationship between Mr. Nosal and KFI began to sour, and Mr. Nosal informed the firm that he was planning to depart. He eventually departed on October 31, 2004.

Prior to his departure, Mr. Nosal negotiated a separation agreement and a companion independent contractor agreement with Peter Dunn, KFI's general

counsel. These agreements contained a variety of provisions. Under the contracts, Mr. Nosal "absolutely" was terminated as a KFI employee, but was to keep working for KFI as an independent contractor in order to complete open searches that he had begun as an employee. (ER 944, 1016-17.) At the time of his departure, he had approximately sixteen open searches. The agreements contemplated that Mr. Nosal would continue to use KFI resources in order to conduct the open searches. Among other things, Dunn understood that although Mr. Nosal himself would no longer have a Searcher password, he would still be able to have KFI employees obtain information from the database for him to complete the open assignments. (ER 620-22, 1033.) On numerous occasions in 2005 while he was working on open searches for KFI, KFI employees forwarded Mr. Nosal documents from Searcher marked proprietary and confidential, including source lists. (*See, e.g.*, ER 1031-34; Def. Ex. C, D, I, J, K; Tr.472-75.)

The separation agreements provided that, upon completing his work as an independent contractor, Mr. Nosal would receive unusually large bonuses in July and October of 2005. (ER 954-55.) The agreements also contained a non-compete provision. It provided that Mr. Nosal would not conduct executive search services for any competing entity for a specified period. (ER 1119, 1123, 1136 [Gov't Exh. 9, section 7(iii)].) (As detailed below in Argument V, the validity of that provision, and the admissibility of evidence concerning it, were very much at issue at trial.)

C. Nosal Partners

Mr. Nosal eventually opened his own business venture, Nosal Partners, an event that ultimately led to both a civil suit by KFI and also to this criminal prosecution. The government presented evidence at trial that, sometime in 2004, Mr. Nosal began discussing the possibility of leaving KFI to start his own firm. He discussed this idea with members of his team—i.e., other KFI employees who worked regularly on his assignments. These included Becky Christian, Mark Jacobson, and Jackie Froehlich-L'Heureaux. Christian, Jacobson, and Froehlich-L'Heureaux were eventually named as co-conspirators, and they testified against Mr. Nosal at trial.

According to Christian's testimony, in one of the initial conversations about starting a new firm, she suggested that they could take information from KFI databases. Mr. Nosal responded: "Don't talk about this in front of me. I don't want to hear it. Talk about it among yourselves." (ER 298.) Christian and Froehlich-L'Heureaux proceeded to begin to download information from KFI's Searcher database. Froehlich-L'Heureaux at one point asked Mr. Nosal where she should store the information, and according to her testimony, he responded, "Figure it out; do what you think is best." (ER 299.) Consistent with his past practice as a high-level executive at KFI, Mr. Nosal himself did not generally access Searcher. And although he did not specifically ask Christian, Jacobson, and Froehlich-L'Heureaux to take information from Searcher, it was their understanding that he wanted them to do so. (ER 305, 334-35, 339, 495-96.)

Christian left KFI in early 2005, a few months after Mr. Nosal had departed. Before she left, she downloaded a variety of information from Searcher. Working with Mr. Nosal, she then set up an executive search firm named Christian & Associates, which was to operate until Nosal Partners could be opened. Under their initial arrangement, Mr. Nosal received 80% of the fees. According to Christian, he also occasionally used a pseudonym, "David Nelson," when meeting with some prospective candidates. (ER 354.)

In March of 2005, Jacobson also left KFI. Like Christian, he intended to join Mr. Nosal's new venture, and like Christian, he downloaded material from KFI databases before he left. Froehlich-L'Heureaux continued to work as an employee for KFI, but she also performed various tasks for Mr. Nosal's new venture. According to her testimony, although she expressed her desire to leave KFI, Mr. Nosal dissuaded her from doing so, at least for a time, and offered to pay her "under the table." (ER 310.)

D. The Internal Investigation and The Referral to the Government

In March of 2005, general counsel Peter Dunn received an email from a fictitious "Sandra Horn" stating that Mr. Nosal was conducting executive searches for KFI clients in Silicon Valley and that KFI would "look like chumps" if they did not sue or otherwise take action against him. (ER 984.) Dunn retained the law firm of O'Melveny and Myers, which had negotiated the settlement agreements, to look into the matter. (ER 986.) In May of 2005, Marlene Briski, an IT specialist at KFI, discovered that Christian, Jacobson, and Froehlich-L'Heureaux had

downloaded a large amount of data from Searcher. KFI began to monitor Froehlich-L'Heureaux's password closely. KFI also hired ex-FBI investigators to go through Christian's garbage and follow Jacobson into his office's lavatory to overhear his conversations. (ER 1053-54.) By early July, KFI had prepared a civil complaint naming Nosal, Christian, Jacobson, and Froehlich-L'Heureaux as defendants.

KFI sought to prompt a federal criminal investigation of Mr. Nosal before the end of July 2005, because the company intended to refuse to pay Nosal (and did not pay him) balloon payments of over a million dollars due in July and October of 2005 for his work as an independent contractor. (ER 1002, 1055.) On July 6, 2005, Sharon Bunzel of O'Melveny's San Francisco office, who had recently left the United States Attorney's Office in San Francisco, contacted Miles Ehrlich, a supervisor in the office. (ER 1054.) On the same day, another O'Melveny attorney sent Ehrlich an email informing him that there were "time sensitive" circumstances that required KFI to file its civil complaint quickly. The attorney included a draft complaint and stated that "we will be able to provide you with additional specific facts that will more than support our position in the complaint and also demonstrate the criminal culpability of those involved." (ER 186-87, 202-04.) The attorney also claimed the value of the downloaded lists was up to $12,000,000. (*Id*.).

On August 2, 2005, based on the information that it had received from KFI, the FBI conducted raids of the San Francisco premises rented in anticipation of

Mr. Nosal opening his new search firm, as well as of the residences of Christian and Jacobson. (ER 1056.)

On the same day as the searches were conducted by the FBI, KFI filed its civil suit. KFI eventually dismissed its suit against Christian, Jacobson, and Froehlich-L'Heureaux on the condition that the three assist the government in any criminal prosecution of Mr. Nosal. (ER 1059-60.) In their trial testimony, KFI officials admitted that it was in KFI's financial interest that Mr. Nosal be convicted in this prosecution. (ER 894, 1057, 1072-73.)

E. The Criminal Charges

The government eventually indicted Mr. Nosal in 2008. The indictment contained substantive charges of computer fraud, trade secret theft, and mail fraud, as well as conspiracy counts. The mail fraud counts were dismissed prior to trial. The remaining batches of counts for computer fraud and trade secret theft are discussed in more detail in the argument section below, and summarized briefly here.

1. Computer Fraud Counts

The government initially alleged eight violations of the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030(a)(4). Five of those counts were based on allegations that Froehlich-L'Heureaux and Christian, while they were KFI employees, had downloaded material from Searcher. The district court dismissed the five "own-password" counts prior to trial, and the government unsuccessfully appealed.

The remaining three counts were "shared-password" counts. They were based on allegations that Christian and Jacobson, after they had left KFI, used Froehlich-L'Heureaux's password to download information from Searcher. The government did not allege that Mr. Nosal himself had conducted any of these downloads—he was charged as an accomplice. After remand from the appeal, the case proceeded to trial, and Mr. Nosal was found guilty on these three charges (Counts Two, Three, and Four), as well as the Count One conspiracy, which alleged the violation of the CFAA as one of its objects.

2. Trade Secret Counts

The Count One conspiracy charge also included as one of its objects the theft of trade secrets in violation of 18 U.S.C. § 1832.[1] The government stipulated that the trade secrets at issue in the conspiracy count consisted of the source lists that were downloaded from Searcher using Christian's, Froehlich-L'Heureaux's, and Jacobson's log-in credentials on nine occasions in 2004 and 2005. Of these nine downloads, only the source lists downloaded on April 12, 2005, by Christian were charged as substantive trade secret offenses (Counts Five and Six).

F. Verdicts and Sentencing

On April 24, 2013, Mr. Nosal was convicted of the three substantive CFAA charges, as well as the two substantive trade secret charges under the EEA. He was also convicted on the Count One conspiracy charge.

---

[1] Prior to trial, the parties agreed that "*particular documents* within that [Searcher] database were trade secrets," not Searcher itself. (See Dkt. 316, Govt.'s Trial Brief at 7 n.2.)

After reviewing extensive documentary evidence, the district court calculated the loss under the Sentencing Guidelines as $46,907. The court concluded that the total value of all nine source lists at issue in the conspiracy charge was not the $12,000,000 reported to the government in July of 2005, or the $434,925.00 to $923,467.50 figures sought by the government at sentencing, but $19,507, based on development costs. (ER 26-30.) The court also added $27,400 in response costs. Based in part on that loss finding, the district court sentenced Mr. Nosal to a term of incarceration of one year and one day. The district court subsequently ordered the defendant to pay $827,983 in restitution, consisting primarily of KFI's attorneys' fees.

ARGUMENT

I. THE CFAA CONVICTIONS MUST BE REVERSED BECAUSE CONSENSUAL PASSWORD SHARING IS NOT AN OFFENSE UNDER THE CFAA

In the *Nosal* en banc decision, this Court adopted a narrow interpretation of the Computer Fraud and Abuse Act. This Court limited the CFAA to hacking crimes, and as a result, it affirmed the dismissal of most of the CFAA counts. After that watershed decision, the case returned to trial, and the government proceeded with a prosecution on several remaining counts, including three CFAA counts. But those counts were based on allegations of consensual password sharing—that one employee allowed another former employee (not Mr. Nosal) to use her password.

That theory is indistinguishable from the theory that this Court rejected in

the *Nosal* en banc decision. Under *Nosal*, the defendant is entitled to acquittal, or at least a new trial, on the remaining counts as well.[2]

A. Procedural Background

1. Charges and Interlocutory Appeal

Mr. Nosal was initially charged with eight counts of violating the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(4). Mr. Nosal moved to dismiss all eight counts for failure to state an offense. He argued that the allegations were based on acts of employee misappropriation, which are not covered by the CFAA.

After this Court's decision in *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127 (9th Cir. 2009), the district court dismissed five of the eight counts. The five dismissed counts were the "own-password" counts—they were based on allegations that Mr. Nosal's alleged accomplices used their KFI passwords to download materials for the new venture. The three remaining counts were the "shared-password" counts—they were based on allegations that Christian and Jacobson used Froehlich-L'Heureaux's password to access Searcher. In sum, the district court dismissed the own-password counts but left standing the shared-

[2] When an argument for acquittal rests on a question of statutory interpretation, the ruling below is reviewed de novo. *United States v. Havelock*, 664 F.3d 1284, 1289 (9th Cir. 2012) (en banc). Challenges to the sufficiency of evidence are also reviewed de novo. *United States v. Carranza*, 289 F.3d 634, 641 (9th Cir. 2002). The evidence must be sufficient that a rational jury could find the defendant's guilt beyond a reasonable doubt. *Jackson v. Virginia*, 443 U.S. 307 (1979). Claims that jury instructions misstate the law are reviewed de novo. *Peralta v. Dillard*, 744 F.3d 1076, 1082 (9th Cir. 2014) (en banc). These standards of review apply to Mr. Nosal's arguments for acquittal and also to his claims that the jury instructions were erroneous. Other applicable standards of review are indicated where appropriate.

password counts.

The government appealed the dismissal of the five own-password counts.[3] A three-judge panel initially reversed the dismissal of those counts, but this Court then heard the matter en banc and affirmed the district court's order. In the *Nosal* en banc decision, this Court held that the CFAA criminalizes "hacking—the circumvention of technological access barriers—not misappropriation of trade secrets." 676 F.3d at 863.

2. Post-Appeal Challenges

After this Court's en banc decision, the case was remanded to district court for trial on the remaining counts. Mr. Nosal renewed his challenge to the three shared-password counts. He argued that under the rationale of the *Nosal* en banc decision, the shared-password counts were also invalid because they did not allege any acts of hacking or circumventing technological access barriers. (Dkt. 276.)

The district court rejected the challenge.[4] It held that the *Nosal* en banc decision did not limit the CFAA to hacking crimes, the term "hacking" was only used in the opinion as "a shorthand term," and the phrase "circumvention of technological access barriers" was merely "an aside." (ER 161.) It further held that some of the explanatory examples given by this Court were mere "dicta."

---

[3] Under this Court's case law, Mr. Nosal was not permitted to cross-appeal the district court's refusal to dismiss the three shared-password counts. *See United States v. Fort*, 472 F.3d 1106, 1121 (9th Cir. 2007).

[4] This case had been before Judge Patel. She retired during the appeal. The case was then re-assigned to Judge Chen.

(ER 162 n.4.) It thus denied Mr. Nosal's motion to dismiss the three shared-password counts.

Mr. Nosal subsequently moved for acquittal under Rule 29. (Dkt. 397, 436.) He reiterated his legal arguments under *Nosal* en banc, and also made additional arguments based on the evidence presented at trial. The district court denied the Rule 29 motions. (Dkt. 455.)

B. Factual Basis of CFAA Counts

The three CFAA counts were based on three downloads from KFI computers in 2005. In each case, Froehlich-L'Heureaux, who was still employed by KFI, provided her KFI password to Christian or Jacobson, who were no longer employed by KFI. Christian and Jacobson then used her password to run searches on behalf of the executive search firm they had founded after leaving KFI. The specific evidence for each count can be summarized briefly.

Count Two - April 12. On April 12, 2005, Christian used Froehlich-L'Heureaux's password to run a search. Christian and Nosal had been retained to find a CFO for WorldHeart, and they anticipated being retained to find a CFO for UTStarcom. In order to facilitate those assignments, Nosal asked Christian to obtain information from the KFI Searcher database. Christian then emailed Froehlich-L'Heureaux and asked to use her password. Christian explained that the searches were complicated, and rather than try to explain the searches to Froehlich-L'Heureaux, Christian asked for her log-in credentials. Froehlich-L'Heureaux provided her password to Christian, who then ran the

searches. Christian then sent the information on April 12 to Nosal in an email. (ER 374-75.)

Count Three - July 12. On July 12, 2005, Christian again used Froehlich-L'Heureaux's log-in credentials to run a search. Christian and Nosal had been working on an executive search for PG&E. While they were both at the new office of Nosal Partners, Christian downloaded information from the KFI database using Froehlich-L'Heureaux's credentials, but Christian testified at trial that she could not remember whether she or Froehlich-L'Heureaux had actually typed in the password to gain entry. Christian downloaded a source list, and subsequently provided the list to Nosal. (ER 718-19.)

Count Four - July 29. On July 29, 2005, Jacobson used Froehlich-L'Heureaux's log-in credentials to run a search. Both were physically present at the Nosal Partners office. Jacobson had been working on an executive search for a motorcycle parts company. He asked Froehlich-L'Heureaux to log in remotely to KFI database using her username and password, which she did. Once logged in, Froehlich-L'Heureaux left, and Jacobson ran searches and downloaded source lists. (ER 313, 500-01.) Jacobson never told Nosal what he and Froehlich-L'Heureaux were doing, Nosal never told him to do it, and Nosal did not know anything about it. (ER 294.)

For each of the three counts, it is undisputed that Christian and Jacobson had Froehlich-L'Heureaux's permission to use her password. The core legal question presented here is whether that sort of computer use constitutes

"unauthorized access" under the CFAA and *Nosal*.

C. Insufficiency

1. Under the CFAA and Nosal, Password Sharing is Not a Crime

As described above, the gist of the CFAA counts is that a current employee allowed a former employee to use her password to access an employer database. Under the *Nosal* en banc ruling, if the current employee had accessed the database herself, there would be no offense. Thus, on July 29th, if Jacobson had asked Froehlich-L'Heureaux to log into the database, then had stood over her shoulder and told her what searches to run, their conduct would not have been covered by the CFAA. According to the government, however, because Jacobson sat down at the computer and ran the searches himself, rather than simply instructing Froehlich-L'Heureaux to run the searches, he committed a federal offense. This is too fine a distinction on which to rest criminal liability.

Put simply, password sharing is not a federal offense. Indeed, it is commonplace and often innocuous behavior. A husband asks his wife to log in to his email and send a document from his home computer; a mother logs in to her daughter's Facebook account to check her postings; a college student logs in to his roommate's Watch ESPN account to watch a football game; a surviving spouse logs in to a decedent's bank account to make transactions. In all such cases, a person uses another's password to access a computer, without the permission of the computer owner. But that does not render the access "unauthorized," and thus criminal, under the CFAA.

a. Applying Nosal

In fact, this Court has already considered the same question presented here. In the *Nosal* en banc opinion, this Court stated that the CFAA cannot be construed to make password sharing a federal offense. It considered the very common situation where a person logs into a social media account using someone else's password, in violation of the user account contract.

> Similarly, Facebook makes it a violation of the terms of service to let anyone log into your account. *See* Facebook Statement of Rights and Responsibilities § 4.8 http://www.facebook.com/legal/terms ("You will not share your password, ... let anyone else access your account, or do anything else that might jeopardize the security of your account.") (last visited Mar. 4, 2012). Yet it's very common for people to let close friends and relatives check their email or access their online accounts. Some may be aware that, if discovered, they may suffer a rebuke from the ISP or a loss of access, but few imagine they might be marched off to federal prison for doing so.

676 F.3d at 861. As this Court recognized in the above passage, the CFAA cannot be reasonably construed to cover such conduct.

Unaccountably, the district court wrote off that passage of *Nosal* as mere "dicta." (*Id*. at 13 n.4.) But this Court has repeatedly warned lower courts against using the "dicta" label to evade the import of binding, published cases. Considered statements in majority opinions constitute law even if they are not strictly and logically necessary to the result. *See United States v. Cassel*, 408 F.3d 622, 633 n.9 (9th Cir. 2005) (citing *United States v. Johnson*, 256 F.3d 895, 916 (9th Cir. 2001) (en banc) (plurality op. of Kozinski, J.)).

Nosal's discussion of password sharing, moreover, was not a mere

rhetorical aside. Rather, it was a straightforward implication of the opinion's core holding: that the CFAA is limited to hacking crimes. The *Nosal* Court held that "Congress enacted the CFAA in 1984 primarily to address the growing problem of computer hacking." 676 F.3d at 858. It rejected the government's contract-based interpretation of the statute, because "[t]he government's interpretation would transform the CFAA from an anti-hacking statute into an expansive misappropriation statute." *Id*. at 857. It concluded by adopting a narrow interpretation of the statute, one where the prohibited conduct consists of "the circumvention of technological access barriers." *Id*. at 963.

Once again, the district court below ignored all of this. It suggested that this Court did not actually mean to limit the CFAA to hacking offenses, and that it only used the word "hacking" as a loose colloquialism, rather than as anything actually limiting the scope of the statute. (Dkt. 314 at 12). That is utterly untrue. The words "hacking" or "hacker" appear a dozen times in the *Nosal* en banc opinion. Its discussions of hacking were not dicta—rather, the core holding of *Nosal* is that the CFAA is limited to crimes of hacking. *See WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199, 207 (4th Cir. 2012) ("[W]e are unwilling to contravene Congress's intent by transforming a statute meant to target hackers into a vehicle for imputing liability to workers who access computers or information in bad faith, or who disregard a use policy.").

Password sharing is not hacking. When Froehlich-L'Heureaux allowed Christian and Jacobson to use her password, she violated KFI's computer use

policy, but she did not commit a federal computer hacking crime. Under *Nosal*, as a matter of law, such conduct does not violate the CFAA.

b. Conferring Authorization

What the *Nosal* opinion recognized is that consensual use of an account holder's password to access a computer is "authorized access." In other words, it is not merely the computer owner who can confer authorization—it is also the password holder. Passwords are keys, and when keys are shared consensually, the resulting entry is not trespassory.

Physical world analogies demonstrate the point. Trespasses occur when there is unauthorized entry into a property. Such unauthorized entries can occur when a person kicks down a door, or picks a lock, or steals a key in order to gain access. But when a key-holder gives her key to another, and that person uses the key to enter the property, the entry is not trespassory. For example, if the son of the owner of a house gives a key to a friend, and the friend uses the key to enter the house, the entry is not a criminal trespass—even though it is done without the owner's consent. *See* Cal. Penal Code § 620(m) (defining criminal trespass as entering or occupying property "without the consent of the owner, *the owner's agent, or the person in lawful possession*" (emphasis added)); *Restatement (Second) of Torts* § 329 (defining as trespasser as "a person who enters or remains upon land in the possession of another without a privilege to do so created by the possessor's consent").

The same principles apply in the virtual world under the CFAA. Access to

computers is often protected by passwords, which serve as keys to access. Unauthorized access occurs when a hacker uses a worm or virus or brute force attack to disable the password protection system—the equivalent of kicking in the door. Unauthorized access also occurs when a hacker steals or guesses another's password and then uses that password to obtain access. But unauthorized access does not occur when the lawful possessor of a password gives her password to another person, and he uses it to access the computer. Such use might violate the password holder's contract or terms of service, but it is not a crime under the CFAA.

To be sure, Congress could write a statute making clear that only the computer's owner, and not a password holder, may confer consent. Congress has not done so. Moreover, to the extent that the current statute is ambiguous as to who may confer authorization, any ambiguity in this regard must be resolved in the defendant's favor. *See United States v. Santos*, 553 U.S. 507, 514 (2008); *see also* Orin S. Kerr, *Computer Crime Law* 48 (2d ed. 2009) (noting that under the CFAA, "there are two parties that have plausible claims to set authorization: the owner/operator of the computer, and the legitimate computer account holder").

But the bottom line is even simpler: In this same case, this Court has already recognized that when a computer account holder shares her password with another person, they do not commit an offense under the CFAA. Under *Nosal*, even though such access may not be authorized by the computer owner, it is authorized by the account holder. It is therefore not a federal crime under the CFAA.

c. Avoiding Overbreadth

The implications of a contrary ruling would be both dramatic and untoward. Password sharing is commonplace, and it is often innocuous or beneficial. Consider some common situations.

Many parents seek to monitor their children's internet use. In order to protect her son, for example, a mother insists that he share his usernames and passwords with her. She then logs into his social media and email accounts to ensure that he is not engaged in anything illicit, and also to ensure that is he not being bullied, harassed, or solicited. In so doing, she would violate the terms of service of Facebook, for example, and she would access Facebook servers without the computer owner's authorization.

Suppose that a dying husband makes a list of his usernames and passwords for financial accounts, and gives the list to his wife. After his death, she uses his passwords to access his accounts in order to manage the affairs of the estate, transfer assets, and shut down accounts. Her conduct is not only innocuous but also entirely necessary, even though it is not authorized by the computer owner. According to the government's interpretation of the CFAA, these two women would be committing federal offenses.

Avoiding such absurd results is precisely why this Court in *Nosal* limited the CFAA to its core conduct: hacking. To hold otherwise—to make consensual password sharing a crime—would render a wide variety of innocuous conduct criminal. Such a broad interpretation is not supported by either the text or the

legislative history of the statute. And in any event, it was already rejected by this Court in the *Nosal* en banc decision.

2. Mr. Nosal Was Authorized to Access KFI Databases

The insufficiency claim presented above is a legal insufficiency claim, which depends on an abstract question of statutory interpretation rather than the facts of this case. The claim is simple: That using an account holder's password with her consent is not an offense under the CFAA. But even if this Court rejects that legal proposition, Mr. Nosal is entitled to acquittal based on the evidence actually presented in this case. The evidence at trial showed that Mr. Nosal, as an independent contractor, was entitled to access information on KFI databases.

Mr. Nosal left KFI and was no longer an employee. But when his employment ended, he and KFI entered into an independent contractor agreement. (ER 1119 [gov't exh. 9].) The gist of the agreement was that Mr. Nosal would continue to work on open executive search assignments, including assignments for Best Buy, Ceridian, and EDS.

Critically, KFI knew and agreed that Mr. Nosal would continue to have access to the Searcher database for the open searches. KFI general counsel Peter Dunn testified that under the independent contractor agreement, Nosal was allowed to receive staffing support from KFI employees, and they could conduct research for him. (ER 1026-30.) And Dunn testified explicitly that he knew that, in order to work on these open assignments, Nosal would have access to the information in the Searcher database.

> Q. Isn't it a fact, at this point, that you understood that Mr. Nosal would be using the resources of Korn/Ferry and Searcher to complete these searches?
>
> [Dunn]: Yes.

(ER 1030.) As Dunn admitted, Mr. Nosal was entitled to obtain any and all information contained in the database—so long as he used it for his open assignments on behalf of KFI. (ER 1032-34.)

What the government showed at trial was that Mr. Nosal obtained information, but then used it for different assignments—assignments that were not for the benefit of KFI. But that simply shows unauthorized *use* of information. That shows misappropriation. What this Court held in *Nosal* en banc is that misappropriation of information is not an offense under the CFAA. Thus, even if password sharing without the computer owner's consent can be a federal offense in some circumstances, it cannot be an offense in the circumstances of this case, where the defendant was entitled to receive the underlying information.

D. Instructions

As argued above, Mr. Nosal is entitled to acquittal because as a matter of law, the conduct proved in this case does not constitute an offense under the CFAA. But even if he is not entitled to acquittal, he is at a minimum entitled to a new trial because the jury instructions failed to describe the law accurately. With respect to the CFAA, the Court instructed the jury:

> Whether a person is authorized to access the computers in this case depends on the actions taken by Korn/Ferry to grant or deny permission to that person to use the computer. A person uses a computer "without authorization" when the person has

> not received permission from Korn/Ferry to use the computer for any purpose (such as when a hacker accesses the computer without any permission), or when Korn/Ferry has rescinded permission to use the computer and the person uses the computer anyway.

(ER 109.) Mr. Nosal objected to this instruction as inconsistent with this Court's ruling in *Nosal*. Quoting that opinion, Mr. Nosal requested that the jury be instructed as follows: "A person accesses a computer without authorization when he circumvents technological access barriers." (Dkt. 373 at 10). But because the district court had written off that language as mere dicta, it overruled Mr. Nosal's objection and refused his instruction. (ER 109.)

The instruction given by the trial court was faulty. In fact, in the critical first sentence, it endorsed precisely the theory that this Court had rejected in *Nosal*. What the first sentence suggests is that any action by the employer can limit authorization. It suggests, in other words, that employer contracts or workplace policies can limit permission, and thus that an employee who accesses a computer in violation of such contracts or policies violates the CFAA. As a matter of law, that is flatly incorrect under *Nosal*. The essential holding of *Nosal* is that *contract-based* limitations on access are insufficient to trigger CFAA liability; rather, only *code-based* limitations on access trigger liability.

As interpreted by *Nosal*, the essential conduct prohibited is "hacking—the circumvention of technological access barriers." 676 F.3d at 863. Mr. Nosal requested that the jury be instructed accordingly. Instead, the trial court instructed the jury that "actions taken by Korn/Ferry" to limit the scope of use and

authorization of information in Searcher were sufficient to create an access barrier and create federal criminal liability. That is untrue. Even if this Court rejects the arguments for outright acquittal, the instructional error merits a new trial.

II. THE CFAA CONVICTIONS MUST BE REVERSED BECAUSE THE GOVERNMENT FAILED TO PROVE THE REQUISITE *MENS REA* FOR ACCOMPLICE LIABILITY, AND THE DISTRICT COURT'S INSTRUCTIONS WERE ERRONEOUS

No evidence was presented that Mr. Nosal used someone else's password to access KFI computers. Rather, the theory of the case was that his co-conspirators had done so, and that Mr. Nosal was liable as an accomplice.

As argued above, the government's theory of the case was legally invalid because password sharing is not a crime under the CFAA. But even assuming *arguendo* that the CFAA covers password sharing, so Christian and Jacobson were guilty as principals, that does not establish Mr. Nosal's liability as an accomplice. Under the Supreme Court's recent decision in *Rosemond v. United States*, 134 S. Ct. 1240 (2014), the evidence was insufficient to prove Mr. Nosal's foreknowledge of password sharing, and the jury instructions were incorrect.

A. *Rosemond*

In *Rosemond*, the Supreme Court clarified the *mens rea* for accomplice liability, an issue that has vexed courts for generations. The defendant was charged with being an accomplice to an offense of using a gun in a drug transaction. The defendant himself did not use a gun, and he disputed that he knew his confederates would use a gun. He claimed that he lacked the requisite intent for accomplice liability.

The Supreme Court started with basic and undisputed propositions: that accomplice liability requires an intent "to facilitate that offense's commission." *Id*. at 1248. That intent "must go to the specific and entire crime charged." *Id*. In other words, a defendant charged as an accomplice must be aware of the criminal nature of the principal's actions. "[F]or purposes of aiding and abetting law, a person who actively participates in a criminal scheme knowing its extent and character intends that scheme's commission." *Id*. at 1249.

But the Supreme Court went on in *Rosemond* to make a new and critically important point: that an accomplice must have *advance knowledge* of the crime that the principal is planning to commit. "[D]efendant's knowledge . . . must be advance knowledge—or otherwise said, knowledge that enables him to make the relevant legal (and indeed, moral) choice." *Id*. An accomplice must know "beforehand of a confederate's design," so that "he can attempt to alter that plan or, if unsuccessful, withdraw from the enterprise." *Id*. In short, what is required for accomplice liability is not just knowledge and presence, but foreknowledge and a decision to provide continued assistance.

B. Insufficiency

The evidence was insufficient to prove intent under *Rosemond*. Even assuming that password sharing is a crime under the CFAA, the government did not prove that Mr. Nosal had advance knowledge that Froehlich-L'Heureaux would share her password with Christian and Jacobson.

The government did present evidence that Mr. Nosal knew and intended that

Christian and Jacobson would obtain information from KFI databases. But there was no evidence presented that he knew *how* they would do so. That fact is critical, as merely obtaining information is not a crime under the CFAA. Put simply, if Mr. Nosal believed that Christian and Jacobson would instruct Froehlich-L'Heureaux to run searches, using her own password, he could not be found guilty of a CFAA offense if they subsequently made a decision—without his knowledge—to borrow her password. If Mr. Nosal believed that Christian and Jacobson would stand over Froehlich-L'Heureaux's shoulder at the computer terminal, he could not be found guilty if they subsequently made a decision—without his knowledge—to take her place at the keyboard. He can only be held liable as an accomplice to illegal password sharing if he knew in advance that there would be illegal password sharing. The evidence showed nothing of the sort.

The trial record contained numerous emails between Nosal, Christian, and Jacobson. Password sharing was never mentioned. Nor in their testimony did Christian or Jacobson recount any conversations where Nosal had instructed them to use Froehlich-L'Heureaux's password, or where they had indicated to him that they were engaged in illegal password sharing. In fact, in the entire trial record, there is only one piece of evidence shedding light on this issue. On redirect examination, the government asked Christian: "Did the defendant know that you were using Ms. Froehlich-L'Heureaux's password after you left Korn/Ferry to get source lists and other documents from Korn/Ferry?" She responded yes. (ER

484.)

But that single piece of opinion testimony is too slender a reed on which to rest this entire CFAA prosecution. First, Christian gave no indication about how she knew that he knew, depriving her opinion of any probative value. Opinion testimony of lay witnesses must be "predicated upon concrete facts within their own observation and recollection-that is facts perceived from their own senses, as distinguished from their opinions or conclusions drawn from such facts." *United States v. Skeet*, 665 F.2d 983, 985 (9th Cir.1982) (internal quotation marks omitted).

Second, and equally importantly, Christian gave no indication about *when* Mr. Nosal obtained this knowledge.[5] If Mr. Nosal only learned of the password sharing after the two allegedly criminal downloads were made, then he is not guilty under the principles announced in *Rosemond*. *See also United States v. Goldtooth*, 754 F.3d 763 (9th Cir. 2014) (reversing defendants' convictions for aiding robbery because there was no evidence that defendants had foreknowledge). The government did not prove, and indeed it did not even attempt to prove, the foreknowledge of illegal password sharing that is necessary for accomplice liability.

//

//

[5] With respect to Count Four, moreover, Jacobson offered no similar testimony that Mr. Nosal was aware of the password sharing.

C. Instructions

But even if the evidence was sufficient to prove that Mr. Nosal knew of and intended to aid password sharing, he is nonetheless entitled to a new trial because the instructions were flawed. The instructions did not require the jury to find the *mens rea* required for accomplice liability. With respect to the knowledge and intent requirement for accomplice liability, the jury was instructed as follows:

> With respect to Counts 2 through 6 of the indictment . . ., you may find that the defendant acted knowingly if you find beyond a reasonable doubt that the defendant:
>
> 1. was aware of a high probability that, [Christian, Jacobson, or Froehlich-L'Heureaux] had gained unauthorized access to a computer used in interstate or foreign commerce or communication, or misappropriated trade secrets, downloaded, copied, or duplicated trade secrets without authorization, or received or possessed stolen trade secrets without authorization, and
>
> 2. deliberately avoided learning the truth.

The government proposed this "deliberate indifference" instruction (Dkt. 319 at 2.) Mr. Nosal objected to it on the ground that the factual allegations in the indictment did not permit a "deliberate indifference' theory of liability. (Dkt. 334, at 3.) The district court overruled the objection and gave the instruction.

The instruction is legally erroneous under *Rosemond*. First, it does not require a showing of advance knowledge, which *Rosemond* held is essential for accomplice liability. In fact, the instruction implies the opposite by placing the act of unauthorized access in the pluperfect tense– i.e., the defendant was aware of a high probability that the others "*had* . . . gained unauthorized access." The

instruction thus permitted the jury to find Mr. Nosal guilty of the CFAA violations if he learned of the acts of unauthorized access after they occurred. Second, even aside from the temporal dimension of foreknowledge, the instruction did not even require actual knowledge. Rather, it essentially set forth a recklessness standard, stating if the defendant was aware of a "high probability" that his cohorts would commit a crime and "avoided learning the truth," he was guilty. That is false under *Rosemond*, which requires intent and actual foreknowledge.

This Court has affirmed a willful blindness instruction for crimes requiring mere knowledge. *United States v. Heredia*, 483 F.3d 913 (9th Cir. 2007) (en banc). The original justification for the concept was based on the Model Penal Code, and its distinction between intent and knowledge. *United States v. Jewell*, 532 F.2d 697, 700-01 (9th Cir.1976) (en banc). Whatever the merits of applying the willful blindness concept to other substantive offenses, it is not a correct statement of the law of accomplice liability, which requires intent. The instruction should not have been given at all in this case, and the error is especially clear after *Rosemond*.[6]

In reversing the defendant's conviction, *Rosemond* held that "the District Court erred in instructing the jury, because it did not explain that Rosemond needed advance knowledge" of the facts constituting his confederate's offense.

---

[6] Mr. Nosal did not object on the basis of *Rosemond*, which had not yet been decided at the time of trial. He nonetheless preserved his claim of error by objecting to the instruction. Regardless, even if a plain error standard is applied, the error is plain, as measured at the time of appeal. *See Henderson v. United States*, 133 S. Ct. 1121 (2013).

134 S. Ct. at 1251. That is precisely what happened in this case as well.

Moreover, even aside from *Rosemond*, the district court erred in this case by including Froehlich-L'Heureaux's name in the instruction. The evidence showed that at all relevant times, Froehlich-L'Heureaux still had a valid password to access KFI computers. If Mr. Nosal believed that she, rather than Christian or Jacobson, had made the downloads, then the jury should have been required to find him not guilty. And yet the instruction told that jury that it could find him guilty regardless of who made the downloads. Especially when combined with the district court's failure to instruct the jury on the substantive requirements of the CFAA, the accomplice liability instruction misstated the law.

The jury instructions in this case informed the jury that it could and should find Mr. Nosal guilty even if he believed that Froehlich-L'Heureaux made the downloads, even if he lacked actual knowledge of her conduct, and even if he only learned about it after the fact. All of those propositions are false as a matter of law. Mr. Nosal is entitled to a new trial with a properly instructed jury.

III THE ELIMINATION FROM THE COUNT ONE CONSPIRACY INSTRUCTION OF THE ELEMENTS OF THE EXISTENCE OF A TRADE SECRET, AND THE DEFENDANT'S KNOWLEDGE OF TRADE SECRET STATUS, REQUIRES THE VACATION OF ALL COUNTS OF CONVICTION

A. Introduction

When an employee takes his employer's property, he commits an act of misappropriation and embezzlement. Such acts are crimes under state law, *see* Cal. Penal Code § 503, and such takings can also be remedied by civil lawsuits.

Federal criminal law, by contrast, covers only a small subset of such conduct. The Economic Espionage Act, 18 U.S.C. § 1832, reaches misappropriation only when the property taken is a trade secret. In passing the EEA, Congress determined that some proprietary information is so critical to the functioning of the national economy that it deserves the extra protection of federal criminal law.

The EEA defines a trade secret as information that the owner has taken measures to keep secret, and that derives independent economic value by virtue of being secret. 18 U.S.C. § 1839(3). In order to establish that information constitutes a trade secret:

> the government must prove three elements: (1) that the information is actually secret because it is neither known to, nor readily ascertainable by, the public; (2) that the owner took reasonable measures to maintain that secrecy; and (3) that independent economic value derived from that secrecy.

United States v. Chung, 659 F.3d 815, 824-25 (9th Cir. 2011).

A modern business's computers contain a great deal of information and intellectual property—e.g., personnel records, accounting data, law review articles downloaded from Westlaw—that, even if considered confidential and proprietary by that company, do not qualify as trade secrets. Taking such material constitutes misappropriation but it does not violate the EEA. *See Buffets, Inc. v. Klinke*, 73 F.3d 965, 969 (9th Cir. 1996) (holding that where defendants misappropriated information but plaintiffs had not protected the information from disclosure, the defendants "may be liable for stealing something, but they cannot be liable for misappropriation of trade secrets").

In this case, the government charged Mr. Nosal with two substantive EEA violations based on downloads of source lists from KFI computers (Counts Five and Six). Mr. Nosal will demonstrate below that the information at issue in Counts Five and Six – lists of publicly available names and contact information – was not a trade secret, and its misappropriation was not covered by the EEA. The downloaded information was publicly available, and all of the data may well have been entered into Searcher without any effort on KFI's part other than setting up the company's website. The same information could have come from, or been located in, the data bases of other major executive search firms. The government offered no evidence to the contrary.

Most importantly, the government failed to introduce any evidence that KFI had not willingly distributed the alleged trade secrets to third parties who were not themselves subject to confidentiality agreements. Nor did the government prove the requisite element of knowledge by the defendant that the information misappropriated was indeed a trade secret.

Precisely because its proof on Counts Five and Six as to the elements of trade secret status and Mr. Nosal's knowledge of that status was so weak, the government sought to lighten its evidentiary burden by eliminating those elements from the district court's instruction on the trade secret prong of the Count One conspiracy charge. The court's flawed instruction to that effect both constructively amended the indictment and deprived Mr. Nosal of his constitutional right to be convicted only upon proof beyond a reasonable doubt of

every element of the charged offense.

B. The Indictment and the Conspiracy Instruction

The indictment alleged theft of actual trade secrets. In the "Method and Means" section of the Count One conspiracy charge, the government alleged again and again that the information which Nosal and his confederates conspired to steal constituted "trade secrets." (ER 1171, para.15: conspirators would "steal...trade secrets from Korn/Ferry's computer system, including source lists and other information;" ER 1172, para. 8: conspirators would "misappropriate Korn/Ferry trade secrets;" *accord* ER 1171, para.: 15-16, ER 1177-1178, paras. 23-25).

Prior to trial, however, the district court indicated that for the conspiracy count, it would not require the jury to find that the source lists actually constituted trade secrets. The defense objected at that time, and again at the close of evidence. But the district court ruled that "the jury . . . may convict Defendant ...of conspiracy even if it finds that the Korn/Ferry source lists at issue here were not trade secrets." (ER 70). It then instructed the jury as follows:

> In Count One of the indictment, the defendant is charged with conspiracy to misappropriate, receive, possess, and transmit trade secrets. ...[I]n order to prove the defendant's guilt beyond a reasonable doubt on the conspiracy charges, the government need not prove the existence of actual trade secrets and that Defendant knew that the information in question was a trade secret. However, the government must prove that Defendant firmly believed that certain information constituted trade secrets.

(ER 261-262).

C. The Constructive Amendment[7]

"A person is entitled under the Fifth Amendment not to be held to answer for a felony except on the basis of facts which satisfied a grand jury that he should be charged." *United States v. Tsinhnahijinnie*, 112 F.3d 988, 992 (9th Cir. 1997). An indictment must be sufficiently specific so as to ensure that a defendant is "prosecuted only on the basis of the facts presented to the grand jury." *United States v. Du Bo*, 186 F.3d 1177, 1179 (9th Cir. 1999)

In *Stirone v. United States*, 361 U.S. 212 (1960), the indictment alleged a Hobbs Act violation based on interference with commerce *entering* the state, but the evidence, the government's closing arguments, and the trial court's instructions permitted conviction on the theory of interference with commerce *leaving* the state. The Supreme Court reversed, holding that, pursuant to the Fifth Amendment's Grand Jury Clause, a defendant may not be convicted on a factual theory of criminal liability different than one on which he was indicted, even if that uncharged theory is supported by the evidence. *See also United States v. Shipsey*, 190 F.3d 1081, 1086-87 (9th Cir. 1999) (applying *Stirone* in reversing defendant's theft convictions).

Here, the grand jury indicted Mr. Nosal on the Count One conspiracy charge on the basis of a conspiracy to steal actual trade secrets. It cannot be said that the grand jury would have indicted on the conspiracy charge if the government had

---

[7] Claims of constructive amendment are reviewed de novo. *United States v. Hartz*, 458 F.3d 1011, 1019 (9th Cir. 2006).

taken the position that (1) Mr. Nosal did not know that the KFI source lists were trade secrets because (2) in fact they were not entitled to trade secret protection. By lifting the requirement that the government prove both the existence of a trade secret and the knowledge of that trade secret, the district court permitted the jury to convict on an impermissible basis: that the alleged coconspirators were guilty on Count One because they "firmly believed" the source lists were trade secrets, even if they were not. The court's instruction constructively amended the indictment and eliminated required elements of the crime charged, an error that cannot be deemed harmless.

D. The *Hsu* Decision

In formulating its instruction, the district court relied on the Third Circuit's decision in *United States v. Hsu*, 155 F.3d 189 (3d Cir. 1998). That case, which did not involve a claim of a constructive amendment, does not support the district court's ruling. In a sting operation, the defendants in *Hsu* tried to purchase the formula for an anti-cancer drug from an undercover agent. They were charged with attempted theft of trade secrets. During pretrial discovery, they sought to obtain the formula for the drug. In an interlocutory appeal of the district court's order denying discovery, the Third Circuit held that in such circumstances, in order to protect the trade secret from disclosure, it need not be provided in discovery. For the same reason, the government did not have to prove actual trade secret status at trial, because that also would have required exposure of the trade secret. Because the defendants were charged only with attempt, the government

needed only to prove that the defendants sought to steal what they firmly believed to be a trade secret. *See* 155 F.3d at 193-94, 202.

The Third Circuit stated explicitly that its ruling was limited to cases where the charges were *only* charges of attempt, and where there was "*no charge of actual theft of trade secrets*." *Id*. at 194. *Hsu*, by its own lights, does not apply here. And if *Hsu* were extended to every EEA case, then the government would never be required to prove actual trade secrets—and the statutory definition of trade secrets would be rendered superfluous. But regardless of the validity or scope of *Hsu*, the simpler point is that the indictment here alleged a conspiracy to steal actual trade secrets, and so the petit jury should have been required to make the same finding.

E. Because the Government Relied Upon a *Pinkerton* Theory of Vicarious Liability, Reversal of Count One Requires that All of Mr. Nosal's Convictions Be Vacated

If the jury convicted Nosal on the basis of the trade secret prong of the Count One conspiracy charge—an outcome consistent with the general verdict on Count One—then it would have been entitled to find him guilty on all five substantive CFAA and EEA charges based on the district court's *Pinkerton* instruction. (ER 253-255 ([instructing the jury on *Pinkerton* liability]).

In its closing argument, the government highlighted the *Pinkerton* instruction, stating that Nosal was liable "for Counts Two through Six, if you find that he was a member of the conspiracy charged in Count One and if one of the members of that conspiracy committed one of those acts in Counts Two through

Six." (Tr. 1622). The government urged jurors to consider the *Pinkerton* instruction "important' because: "The basis for Mr. Nosal's liability is that he was involved in a conspiracy with other individuals, and that those acts were a natural and probable consequence of that conspiracy." *(Id.)* Thus the constructive amendment of the trade secret prong of Count One in itself requires that all six counts be vacated.[8]

IV. THE TRADE SECRET CHARGES MUST BE DISMISSED BECAUSE THE GOVERNMENT DID NOT PROVE THAT THE DOWNLOADED INFORMATION WAS A TRADE SECRET, NOR DID IT PROVE THE REQUISITE ELEMENTS OF KNOWLEDGE AND INTENT

A. Counts Five and Six

Mr. Nosal is also entitled to acquittal on the substantive trade secrets counts because the government failed to prove that the source lists taken were actually trade secrets.

Count Five charged that on April 12, 2005, Christian used Froehlich-L'Heureaux's login credentials to get documents from KFI's computer to be used in her search for a CFO for UTStarcom. This was the same download charged as a CFAA violation in Count Two. Christian emailed the information on to Nosal in an email with three attachments alleged to be trade secrets. The attachments were source lists for a CalMicro search and two Perkins Elmer searches. (ER 1101-

[8] Likewise, due to the government's reliance on the *Pinkerton* theory, the errors which marred the CFAA substantive charges and the CFAA prong of the Count One conspiracy (*see* Arguments I and II) require reversal of not only Counts One to Four, but Counts Five and Six as well.

1118) . Nosal had been involved in those searches while employed at KFI. (ER 374-377; 542-544, 632). The information contained in the three source lists contained only names of candidates, their company positions, and some telephone numbers. (ER 633-634).

There was no testimony that Christian ever had a subsequent discussion with Mr. Nosal about his receipt of the April 12th email or the three attachments. There was forensic evidence that the email was opened, but there was no way to tell whether the attachments were ever opened. (Tr. 1404-1406). Three names from the lists were forwarded to UTStarcom, and one, Fran Barton, was placed with the company.

Count Six was based on theft of alleged trade secrets for use in the World Heart CFO search. It was based on the same three source lists in Count Five, as well as a "cut and paste." Again on April 12th, Christian logged onto Searcher using JFL's login credentials, ran a query for the World Heart CFO search, and cut and pasted names from the query into two emails to Nosal. (ER 365-367) The names on the cut and paste were part of an active, open assignment at KFI for another company, in which Nosal was not involved. (ER 553-554). A hard copy of one of the two emails was found in Christian's home which had Nosal's handwriting on it and had the name of Michael Pfeiffer circled. (ER 370, 1090). On May 3, 2005, Christian sent Pfeiffer's resume to the CEO of World Heart. (ER 370-371).

//

B. The Law of "Trade Secrets"

"Indispensable to an effective allegation of a trade secret is proof that the matter is, more or less, secret. In the absence of secrecy the property disappears." 1 *Milgrim on Trade Secrets* § 1.03 (2012) (footnotes omitted); *see Ruckelshaus v. Monsanto Co.*, 467 U.S. 986, 1002 (1984). As the Supreme Court has stated, federal trade secret law "functions relatively as a sieve," as it provides far weaker protection than patent law. *Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470, 476 (1974). Displaying supposed trade secrets as advertising to potential customers undermines trade secret status. 1 *Milgrim*, *supra,* § 1.05[2] ("[A] trade secret may be lost through disclosure occurring in advertising, trade circulars, or in an analogous manner."); *see McKay v. Communispond, Inc.*, 581 F. Supp. 2d 801 (S.D.N.Y. 1983) (holding voluntary disclosure destroys trade secret status). Furthermore, "[i]t is well recognized that a trade secret does not offer protection against discovery by fair and honest means such as...accidental disclosure." *Chicago Lock Co. v. Fanberg*, 676 F.2d 400, 404 (9th Cir. 1982).

Nearly every reported judicial decision involving a criminal prosecution under § 1832 involves a trade secret whose protection, unlike those alleged here, is intended to promote scientific progress. *See, e.g.*, *United States v. Yang*, 281 F.3d 534, 540-44 (6th Cir. 2002) (scientific information about adhesives research).[9]

---

[9] *See also United States v. Krumrei*, 258 F.3d 535, 536-37 (6th Cir. 2001) ("new process for applying hard coatings to the laminate contact surfaces of caul plates"); *United States v. Martin*, 228 F.3d 1, 8-10 (1st Cir. 2000) (composition of veterinary diagnostic tests and research-and-development data); *United States v.*

As a general rule, customer lists are not sufficiently secret to constitute trade secrets. "[T]he customer list cases stand on the periphery of that area of the law which can best be described as the 'trade secret quagmire'." *Zoecon Indus. v. American Stockman,* 713 F.2d 1174, 1179 n.9 (5th Cir. 1983) (internal quotation marks omitted); *see also Nationwide Mut. Ins. Co. v. Mortensen*, 606 F.3d 22, 28 (2d Cir. 2010) (noting that while customer lists can be "trade secrets," they "lie on the periphery of the law of trade secrets") (internal quotation marks omitted); 1 *Milgrim*, *supra*, § 1.09[7]. In order for a plaintiff to possibly qualify a customer list for trade secret protection, a case-specific showing must be made both as to secrecy and the time and effort required to compile the list. *See Retirement Group v. Galante*, 176 Cal. App. 4th 1226, 1240 (2009).

C. The Government Failed to Prove the Information at Issue in Counts Five and Six Constituted Trade Secrets

1. Customer Lists and Difficulty Of Development

The information at issue in Counts Five and Six, consisting of 374 names with associated phone numbers, and company titles, were even less susceptible to trade secret treatment than customer lists.[10] It is undisputed that most of the information contained in Searcher consisted of information from public sources. .

Hsu, 155 F.3d 189, 191-92 (3d Cir. 1998); *United States v. Genovese*, 409 F. Supp. 2d 253, 255 (S.D.N.Y. 2005) (source code).

[10] Given the court's determination at sentencing that the placement of a 5,649 names on nine KFI source lists involved development costs of $19,507.88, or less than three and a half dollars per name (ER 26-30), the value of the lists at issue in Counts Five and Six containing 374 names would have been under $1,300.00.

(ER 413-18, 475, 582, 881.) Marilyn Briski, KFI's IT expert, as well as Christian and Jacobson all testified unequivocally that the data in Searcher came from public sources like the Wall Street Journal, the New York Times, Hoovers, Zoom Info, LinkedIn, Google, corporate websites, etc. (ER 413-418, 475, 582). "Thousands and thousands" of publicly known names, resumes, and cell phone numbers simply sailed in over KFI's transom by means of its website and then were input into Searcher. (ER 585). KFI employees inputted information into Searcher regarding people they met at cocktail parties or knew from prior jobs. (ER 839-875). Since it was impossible to determine where data in a Searcher came from (ER 877-878, 882; 610-613), all of the information at issue in Counts Five and Six could have come from public sources. No witness testified how these specific lists were put together, what efforts or resources went into creating these lists, or what resources were culled for the information.

Anyone seeking a list of CFOs can go to Google, type in "United States CFOs," and download hundreds of names, companies, and positions in a few minutes. Assume that KFI downloaded into Searcher the 2004 and 2005 list of the "America's Best CFOs" published in each of those years by the "Institutional Investor" magazine, a not unlikely event, as much of the information on potential candidates in Searcher came from public sources such as publications. (ER 881, 413, 475, 582). The Institutional Investor lists would then be automatically marked "KFI Proprietary and Confidential," as was true of all the contents of Searcher. (ER 851). But as the Institutional Investor lists are publicly available

documents, they could not qualify as trade secrets as a matter of law.

As has been said of customer lists, "lists containing merely public information that can easily be compiled by third parties will not be protected as trade secrets" unless the compiler "expends a great deal of time, effort and expense in developing the lists." *Fireworks Spectacular, Inc. v. Premier Pyrotechnics, Inc.*, 147 F. Supp. 2d 1057, 1062-63, 1066 (D. Kan. 2001). Absent proof that the three CFO lists and the "cut and paste" specifically at issue in Counts Five and Six represented any meaningful KFI work product, the information could not qualify as a KFI trade secret. *American Paper*, 183 Cal. App. 3d at 1326.

Information brought by employees from prior employers also cannot constitute a trade secret. The government offered no evidence that the information in question had not been brought to KFI by one of its many new hires from Spencer Stuart or other executive search companies. (ER 423). Indeed, because it was conceded that Nosal himself had worked on the earlier Cal Micro and Perkins Elmer searches, the government was obliged to prove that the names on the source lists were not information that he had brought with him from his prior search firm.

It is possible to imagine a source list, consisting of far more than publicly available data, which a search firm expended substantial expenditure of time and money to compile.[11] But the government failed to prove that the specific

[11] Indeed, there was evidence in this case that KFI sent Nosal confidential documents containing substantial work product in connection with the open searches he was conducting for Best Buy and EDS. Defense Ex. C was a list of over 150 candidates for the Best Buy CIO search with notes on the status and

information in question in Counts Five and Six was the product of "a great deal of time, effort and expense" on the part of KFI, and thus failed to prove it qualified as a trade secret.

2. Actual Secrecy

The government also faced the heavy burden of proving beyond a reasonable doubt that the source lists for which it claimed trade secret status were "*actually secret* because it [was] neither known to, nor readily ascertainable by, the public." *Chung*, 659 F.3d at 824 (emphasis added). Given KFI's treatment of its source lists, the law also imposed on the government the burden of proving non-disclosure as to any information alleged to be a trade secret. In finding that a customer list left on a computer that had been sold could not constitute a trade secret of the former owner of the computer, the Second Circuit stated: "[T]he owner is entitled to such protection only as long as he maintains the list in secrecy; upon disclosure, even if inadvertent or accidental, the information ceases to be a trade secret and will no longer be protected." *Defiance Button Machine Co. v. C&C Metal Products Corp.*, 759 F.2d 1053, 1063 (2nd Cir. 1985).

The government's own witnesses established that, once source lists were created, they were not password-protected. Nothing prevented them from being shared outside KFI. (ER 426-429). Source lists were disclosed or sold to clients during pitches and in "mapping" engagements. (ER 590). The source lists being

---

evaluation of each candidate. Defense Ex. Q, a list for the Best Buy CIO Search, contained status notes regarding each candidate. None of these far more detailed documents, of course, was alleged to have been a trade secret stolen by Nosal.

used in a given search were given to clients who asked for them. Christian testified that KFI employees regularly emailed source lists around, took them home, gave them to clients and so on. (ER 421-423). It was common in the industry for people, including people at competing firms, to share information. (Tr. 1196-98). Employees were free to take all their source lists with them when they left KFI; no measures to prevent such public dissemination, such as exit interviews or demands for the return of the material, were in place. Under this Court's decision in *Buffets*, that alone undermines trade secret status. 73 F.3d at 969.

"If an individual discloses his trade secret to others who are under no obligation to protect the confidentiality of the information, or otherwise publicly discloses the secret, his property right is extinguished...." *Ruckelshaus*, 467 U.S. at 1002. Here, the government failed to offer any proof that the Cal Micro and Perkins Elmer lists and Sirna "cut and paste" information had not been disclosed without confidentiality protections to those clients themselves, as the government's witnesses testified sometimes occurred in the course of searches. (ER 903). Given the nature of the source lists at issue in Count Five, which were bereft of any information of the sort produced by a meaningful investigation of candidates, proving secrecy was virtually impossible—which no doubt explains why a source list has never been judicially found to constitute a trade secret. This should not be the first case to do so.

//

//

D. The Government Failed to Prove Knowledge of Trade Secret Status

In addition to proving actual trade secret status, the government was also required to prove Mr. Nosal's knowledge of trade secret status. (ER 256-258). Given that the government failed to prove that the source lists in Counts Five and Six were trade secrets, it necessarily failed to prove that Nosal or Christian knew them to be trade secrets.

Furthermore, despite being the government's key witness on the Count Five and Six charges, Christian, the person who downloaded the lists at issue, never testified that either she or Nosal were familiar with the definition of a trade secret or that they believed the downloaded material to be entitled to trade secret protection. Nor would such a belief have been well-founded. Christian well knew that source lists frequently contained nothing but public information and were commonly disclosed to outside parties. Mr. Nosal would have known the same. Nor would he consider lists of names from executive searches he himself had conducted to be trade secrets.

In closing argument, the government hung its hat on this knowledge element on one piece of evidence. That is, the agreements employees signed when hired at KFI, including Nosal, stated that a variety of information, including source lists and position specifications, is confidential KFI information and is afforded the legal protection of trade secrets. (ER 914-916). But mere labels do not a trade secret make. As the trial court correctly instructed the jury, "just because a document refers to information as a trade secret, confidential, or proprietary, does

not necessarily make that information a trade secret." (ER 259-260). *See Glaxo Inc. v. Novopharm Ltd.*, 931 F. Supp. 1280, 1302 n.23 (E.D.N.C. 1996) ("Stamping a document 'confidential' does not make the information contained therein so.").

Furthermore, the clause in the KFI confidentiality agreement is demonstrably false. Another clause in the same agreement states that information brought to KFI by new hires is not confidential, nor is information disclosed to the public. Since many source lists in Searcher fit these descriptions, they are not "afforded the legal protection of trade secrets," despite KFI's ipse dixit to the contrary.

E. The Government Failed to Prove Knowledge of, or an Intent to, Injure KFI

Finally, the reach of the provisions of the EEA herein at issue is limited to situations in which the party who misappropriates information does so for the purpose of using that information to the detriment of the trade secret holder. For that reason, the offense requires the additional element of knowledge of injury or an intent to injure the holder of the secret. (ER; 8 RT 1584-1585). The element of a defendant's knowledge of injury is an important safeguard against the wrongful expansion of federal criminal liability to reach matters of economic insignificance that can be dealt with through state judicial or administrative proceedings.

The record contains no evidence that Mr. Nosal or Christian acted with such intent or knowledge in downloading the Cal Micro and Perkins Elmer lists or the "cut and paste" information. Christian testified that three names from the source

lists were forwarded to UTStarcom, and one of the three was ultimately placed. But the government introduced no evidence to suggest that Nosal's work on the UTStarcom search in any way did, or could have, caused economic injury to KFI, a billion dollar corporation, much less that the use of the names could have caused such injury. There is not a shred of evidence in the record to support a claim that Nosal or Christian *knew* that the downloading of the list would cause such injury.

Likewise, there was no evidence that either Nosal or Christian knew that the downloading of the cut and paste list could or would injure KFI. The download resulted in the sending of a single name to World Heart, which already had retained Christian for its CFO search.

For all of these reasons, Nosal is entitled to acquittal on Counts Five and Six.

F. The Court Committed Reversible Error by Giving its "Deliberate Indifference" Instruction as to Counts Five and Six

For the trade secrets counts, the government had to prove beyond a reasonable doubt that Mr. Nosal knew that the information downloaded by Christian constituted a trade secret. If he knew that the downloads were taking place, but did not know that the lists were trade secrets, then he was not guilty of the charged offenses. Additionally, under *Rosemond*, in order to establish Mr. Nosal's liability as an aider and abettor, the government was required to prove that his knowledge of the trade secret status *preceded* the actus reus of the charged offenses. *Rosemond*, 134 S. Ct. at 1249.

The district court did instruct the jury that knowledge of trade secret status was a necessary element of Counts Five and Six (ER 257-258), but then contradicted that message by instructing that actual knowledge need not be proven if "deliberate indifference" was proven instead. (ER 263-264). As Mr. Nosal demonstrated in Argument II. C. with respect to the CFAA counts, the deliberate indifference instruction was erroneous under *Rosemond*. That argument applies equally to the EEA counts. Under *Rosemond*, actual advance knowledge is required for accomplice liability, and deliberate indifference is not sufficient. Thus, were this Court to reject defendant's preceding arguments for acquittal on Counts Five and Six, Mr. Nosal would be entitled to a new trial based on the instructional error.

V. THE DISTRICT COURT COMMITTED REVERSIBLE ERROR IN ADMITTING IRRELEVANT OPINION EVIDENCE CONCERNING THE NON-COMPETE COVENANT BUT EXCLUDING CONCLUSIVE EVIDENCE THAT THE PROVISION WAS LEGALLY VOID

A. The Role of the Non-Compete Agreement at Trial

As initially indicted, the cornerstone of the government's case rested on the allegation that Mr. Nosal had defrauded KFI by accepting monthly payments for his work as an independent contractor, while violating the provision of his separation agreement barring him from participating in any non-KFI executive searches during the contract period. In challenging the initial indictment, Mr. Nosal relied on black letter California law prohibiting the imposition of non-compete agreements on former employees and independent contractors, and

declaring such covenants void *ab initio*.[12]

Despite the pretrial dismissal of all the mail fraud charges, at trial the government sought to introduce the non-compete provision as a centerpiece of its case on the theory, *inter alia*, it was "probative of whether [Nosal] possessed an intent to defraud Korn/Ferry with respect to the charged offenses" (Dkt. 303 at 13-15). The government sought an order "preclud[ing] Nosal from introducing evidence or argument that the Nosal-Korn/Ferry Agreements, or any portions thereof, were 'illegal,' 'void,' or unenforceable." (*Id*. at 15). Mr. Nosal responded that: the restrictive covenants were clearly void from inception; he never had any legal obligation to honor them; the Court should issue an order to that effect or, alternatively, permit the parties to present to the jury evidence and argument on their competing positions and then instruct the jury on the governing principles of California law. (Dkt. 313 at 5-13). Mr. Nosal alternatively proposed that the court bar from admission any and all evidence concerning, or reference to, that provision in Nosal's separation agreements. (Dkt. 344 at 1-6).

In its Final Pretrial Conference Order (ER 129-150), the court ruled that (1) either party could introduce evidence of a person's subjective belief about the validity of the non-compete clause where relevant and otherwise admissible under Fed.R.Evid. 403; (2) the government could not argue "that Defendant's breach of the agreement is probative to his motive or intent to defraud;" and (3) neither party could introduce evidence or offer argument about whether the non-compete clause

[12]*See Edwards v. Arthur Andersen LLP*, 44 Cal. 4th 937, 945 (2008) ("Today in California, covenants not to compete are void....").

was actually legal and enforceable. (ER 134-136)

As a result of the Court's ruling, the jury heard extensive testimony to the effect that Nosal had breached the non-compete agreement. In addition to hearsay evidence from multiple emails from "Sandra Horn" accusing Nosal of dishonesty, Peter Dunn testified that in 2005, KFI stopped making payments to Nosal under the separation agreements because : "We had reason to believe that he was in breach of those agreements and his obligations." (ER 1001-1003). When Dunn was asked whether non-competition agreements are illegal in some states, however, the court sustained an objection on relevance grounds. (ER 1024-1025).

Christian testified that with respect to Mr. Nosal doing "other kinds of search work after he left" KFI, he had a "nonsolicitation agreement, and he's not allowed to conduct searches outside of Korn/Ferry once he left." (ER 342). According to Christian, in dealing with new clients, he sometimes used the name "David Nelson," "[b]ecause he didn't want people to know that he was conducting search work, which would breach his contract with Korn/Ferry." (ER 354-355). Mark Jacobson understood that according to Mr. Nosal's separation agreement, he was not to compete with KFI for approximately one year. (Tr.1099).

The district court instructed the jury that whether "Mr. Nosal breached or did not breach this covenant is not relevant to the question of whether he is guilty of the crimes charged in this case." (ER 247-248). Nonetheless, in its rebuttal closing argument, the government argued that the fact that Mr. Nosal used the name "David Nelson" and hid his identity proved that there was a crime and that

Nosal's "intent was to conspire with Becky, with Mark, and with Jackie to steal info, some of which was trade secrets, but to steal information from Korn/Ferry...." (ER 226).

B. Argument

The district court correctly instructed that evidence that "Mr. Nosal breached or did not breach this covenant is not relevant to the question of whether he is guilty of the crimes charged in this case." (ER 247-248). That being the case, all evidence concerning the non-compete provision should have been excluded from admission, as the defense requested.[13]

Instead, the court permitted the admission of extensive evidence from prosecution witnesses Dunn and Christian, as well as inflammatory hearsay statements from the fictitious "Sandra Horn," that Mr. Nosal dishonestly breached the non-compete covenant. Yet the court barred the defense from establishing that the provision was illegal under California law and thus void *ab initio*. Such conflicting and unfair evidentiary rulings can constitute grave error. *See United States v. Waters*, 627 U.S. 345, 357 (9th Cir. 2010) (holding that trial court's evidentiary rulings were an abuse of discretion where they provided jury with one-sided picture of defendant by allowing government to rely on "other acts" evidence to establish that she supported a radical environmental organization while prohibiting her from rebutting that evidence with evidence of her contrary

[13] A district court's rulings regarding the admission and exclusion of evidence are reviewed for abuse of discretion. *United States v. Curtin*, 489 F.3d 935, 943 (9th Cir. 2007) (en banc).

values).

Although the court ruled pretrial that the government could not argue "that Defendant's breach of the agreement is probative to his motive or intent to defraud" (ER 226), in its rebuttal closing argument, the government did just that. According to Christian, Nosal used the name "David Nelson" because of the constraints of the non-compete agreement. The government argued to the jury that the use of a pseudonym proved there "was a crime" and showed that Nosal's "intent was to conspire with Becky, with Mark, and with Jackie to steal info, some of which was trade secrets, but to steal information from Korn/Ferry...." (ER; 8 RT 1689). Given the weakness of the evidence of the charged crimes, the government's reliance on irrelevant but highly prejudicial opinion evidence to convict was not harmless.

VI. THE RESTITUTION ORDER MUST BE VACATED BECAUSE IT WAS GROSSLY DISPROPORTIONATE TO LOSS AND BECAUSE IT INCLUDED ATTORNEYS' FEES THAT WERE NOT PROXIMATELY CAUSED BY THE DEFENDANT'S OFFENSES

Unlike the usual case of theft or misappropriation, where the victim is left without something of value after the offense, in this case the offense conduct caused no damage to the Searcher database and did not disable it or render it less useful to KFI. In part as a result, the parties disputed how loss should be calculated, both under the Sentencing Guidelines and also under the Mandatory Victim's Restitution Act (MVRA), 18 U.S.C. § 3663A. The district court ultimately calculated a Guidelines loss of $46,907. Incongruously, however,

several months later the court calculated a restitution award of $827,983. The restitution award was thus nearly twenty times greater than the actual loss amount under the Guidelines.

The district court's restitution award must be reversed for two reasons.[14] First, the award was grossly disproportionate to the actual loss under the Guidelines. Second, the award included $595,758.25 in attorney's fees expended by KFI to pursue Mr. Nosal, and those fees were not reasonable, not necessary, and not proximately caused by the offense conduct.

A. Trial Court's Rulings

For the Sentencing Guidelines offense level, the government proposed a loss of hundreds of thousands of dollars based on KFI's supposed "response costs," as well as KFI's own estimates of how much time and money it would take to re-create the executive source lists that Christian and Jacobson had taken for Mr. Nosal. (See Dkt. 476). These estimates were based on a variety of assumptions that ranged from questionable to almost laughable—they included, for example, KFI's "overhead costs" that had nothing to do with the source lists, and KFI's estimates that those who produced content for Searcher had an average annual compensation of over $400,000, while evidence showed that the actual compensation was generally a little over $80,000 per year.

The trial court rejected most of the government's arguments. It calculated

[14] Interpretation of a restitution statute, and the legality of a restitution order, are reviewed de novo. Restitution awards are otherwise reviewed for abuse of discretion. *United States v. Lazarenko*, 624 F.3d 1247, 1249 (9th Cir. 2010).

an actual loss under Guidelines § 2B1.1 of $46,907. (Dkt. 503). That figure was based on investigation costs of $27,400 and development costs of $19,507.

The district court then requested additional argument and evidence regarding restitution under the MVRA. Several months later, it issued a restitution order requiring Mr. Nosal to pay KFI $827,983 in restitution, more than twenty times the actual loss amount. (Dkt. 547). The bulk of that award was based on attorneys' fees that KFI had paid to O'Melveny & Myers in the ten years since the offense conduct. (*Id*. at 8-13). That restitution award was legally flawed under this Court's case law. It must be vacated.

B. Relationship Between Guidelines Loss and Restitution Loss

Both a defendant's sentence under the Guidelines and a restitution award are based on loss to the victim. *See* U.S.S.G. § 2B1.1(b) & application note 3; 18 U.S.C. § 3663A(b). The two concepts are closely related.

This Court has previously held that a restitution award may not exceed a Guidelines loss calculation. *United States v. Stoddard*, 150 F.3d 1140 (9th Cir. 1998). In *Stoddard*, the district court calculated actual loss under the Guidelines of $30,000, but it then ordered restitution under the Victim and Witness Protection Act (VWPA), 18 U.S.C. § 3663, of over $116,000. *Id*. at 1145-47. This Court reversed the restitution award. It held: "Restitution can only be based on actual loss." *Id*. at 1147. It thus remanded the case "for resentencing on the issue of restitution based on actual loss of $30,000." *Id*.

While *Stoddard* interpreted the VWPA rather than the MVRA, this Court has held that "the VWPA and the MVRA are identical in all important respects, and courts interpreting the MVRA may look to and rely on cases interpreting the VWPA as precedent." *United States v. Peterson*, 538 F.3d 1064, 1075 n.6 (9th Cir. 2008) (internal quotation marks omitted). As to the relationship between the Guidelines and the restitution statutes, there is no textual difference between the VWPA and the MVRA that would command a different result. Nor has this Court questioned or overruled *Stoddard*. In fact, it has repeatedly cited *Stoddard* with approval. *See, e.g., United States v. Xu*, 706 F.3d 965, 994 (9th Cir. 2013) ("Restitution can only be based on actual loss.") (quoting *Stoddard*).

The government itself conceded the *Stoddard* rule at the outset of the sentencing proceedings, stating that "that restitution awarded under VWPA may not exceed Guidelines loss amount." (*See* Govt. Supp. Sentencing Memo. at 20). But then it backtracked and convinced the district court to ignore *Stoddard*.

It is true that a restitution award may not always equal a Guidelines loss calculation. This Court has warned that trial courts should not automatically rely on Guidelines loss to set a restitution award. *Xu*, 706 F.3d at 993-94. But that is because the Guidelines award will usually be greater than the allowable restitution award, for two reasons. First, Guidelines loss includes loss from both the offense conduct and also other relevant conduct, whereas restitution awards include loss only from the offense conduct. *See Hughey v. United States*, 495 U.S. 411, 417-20

(1990). Second, Guidelines loss can be based on either actual loss or intended loss, whereas restitution awards may only be based on actual loss.

Thus, a Guidelines loss calculation is often larger than a restitution award. But the "opposite is impossible: because courts must rely on the greater of intended or actual loss to calculate a guidelines sentence, a restitution order should never exceed the loss used to calculate a sentence." *United States v. Dokich*, 614 F.3d 314, 320 (7th Cir. 2010). Under that principle, the district court's restitution award in this case was illegal, and this case should be remanded for a restitution award that is no greater than the Guidelines loss.

Even if a restitution order may in some cases exceed Guidelines loss, it must be reasonably proportionate to the loss. For example, this Court has rejected Eighth Amendment challenges to restitution statutes precisely because restitution awards are supposed to be proportionate to actual losses. "Where the amount of restitution is geared directly to the amount of the victim's loss caused by the defendant's illegal activity, proportionality is already built into the order." *United States v. Dubose*, 146 F.3d 1141, 1145 (9th Cir. 1998) (internal quotation marks omitted).

If restitution is entirely de-coupled from Guidelines loss amounts, then the restitution statutes will quickly run into constitutional difficulties, a result to be avoided. *See Clark v. Martinez*, 543 U.S. 371, 380-81 (2005). The restitution statutes must be interpreted such that restitution awards are at least proportionate to actual loss. *See Paroline v. United States*, 134 S.Ct. 1710, 1729 (2014) ("To be

sure, the statute states a strong restitutionary purpose; but that purpose cannot be twisted into a license to hold a defendant liable for an amount drastically out of proportion to his own individual causal relation to the victim's losses.").

The district court's restitution award in this case did not merely exceed the actual loss—it exceeded it by nearly twenty times and is therefore illegal under *Stoddard* and the MVRA.

C. Attorneys' Fees

The restitution award in this case must also be vacated because it included hundreds of thousands of dollars of corporate attorneys' fees that were neither reasonable nor necessary nor proximately caused by the defendants' conduct.

The Supreme Court has held that the restitution statutes "limit[] restitution to those losses proximately caused by the defendant's offense conduct." *Paroline*, 134 S. Ct. at 1719. This Court has agreed. *United States v. Gordon*, 393 F.3d 1044, 1057 (9th Cir. 2004) (only costs that are a "'direct and foreseeable result' of the defendant's wrongful conduct" may be included in a restitution award).

The Supreme Court in *Paroline* did not offer a definition of proximate causation, but stated that the concept should be defined as it has elsewhere in both tort law and criminal law. In other contexts, the Supreme Court has held that proximate causation does not include all harms that are foreseeable from a defendants' conduct, but instead requires "the existence of a sufficiently 'direct relationship' between the fraud and the harm." *Hemi Group, LLC v. City of New York*, 557 U.S. 1, 12 (2010). In related contexts regarding loss and causation, this

Court has held that "direct" means "follows as an immediate consequence of the defendant's activity." *United States v. LSL Biotechnologies*, 379 F.3d 672, 680 (9th Cir. 2004).

Because restitution is limited to loss or harm proximately caused by the defendant's conduct, it ordinarily does not cover attorney's fees.[15] *See United States v. Papagno*, 639 F.3d 1093 (D.C. Cir. 2011) (corporate entity's internal costs not recoverable under the MVRA because they are not incurred as a necessary result of the defendant's conduct); *see also United States v. Waknine*, 543 F.3d 546, 559 (9th Cir. 2008) (vacating a restitution award and instructing that attorneys fees may only be awarded where "reasonably necessary"). Instead, this Court has held that attorneys' fees can be recovered under the MVRA only in limited situations such as when incurred in the immediate aftermath of discovery. *United States v. Gordon*, 393 F.3d 1044, 1056-58 (9th Cir. 2004); *see also United States v. Abdelbary*, 746 F.3d 570, 577 (4th Cir. 2014) (stating that attorneys' fees may be recoverable in "exceptional scenario[s]"); *United States v. Elson*, 577 F.3d

[15] The district court here awarded attorneys' fees under subdivision (b)(4) of the MVRA. That provision states that a court must order a defendant to "reimburse the victim for lost income and necessary child care, transportation, and other expenses incurred during participation in the investigation or prosecution of the offense or attendance at proceedings related to the offense." 18 U.S.C. § 3663A(b)(4). The provision was added to the restitution statutes as part of the Violence Against Women Act. *See* Pub. Law 103-322 § 40504 (1994). Its stated purpose was to allow individual victims of "sexual exploitation" to recover expenses for their participation—such as child care expenses and travel expenses incurred while they testified at trial. S. Rep. 103-138 at 6. Subdivision (b)(4) did not mention attorneys' fees for corporate victims.

713, 728 (6th Cir. 2009) (describing the line between ordinary cases, where attorneys fees are not recoverable, and unusual scenarios where they are).

The massive award of attorneys' fees in this case was legally invalid. Unlike the fees awarded in *Gordon*, the fees here were not necessary to determine the scope of the defendants' conduct in the immediate aftermath of discovery. Rather, the bulk of the fees in this case were incurred years after discovery, as part of KFI's ongoing cooperation with federal prosecutors—as well as its closely related pursuit of Mr. Nosal in civil proceedings. (See Dkt. 547 at 8 (awarding attorneys' fees incurred "between the months of July 2005 through January 2014").)

Nor were the fees proximately caused by Mr. Nosal's conduct. They were not necessary, and they did not follow directly from—i.e., as an immediate consequence of—the alleged offense conduct. *See Paroline*, 134 S. Ct. at 1719 (holding that under principles of proximate causation, "there must be some direct relation between the injury asserted and the injurious conduct alleged"). The fees in this case included such tasks as reviewing this Court's ruling in the *Nosal* en banc opinion, which was issued seven years after the offense conduct, and only occurred due to the government's decision to pursue an interlocutory appeal. Those "losses" were not directly caused by Mr. Nosal, and awarding such attorneys' fees to a corporation also represents an utter perversion of the MVRA, and particularly to the provision passed to protect individual victims of sex crimes.

In sum, there was no direct relationship between Mr. Nosal's conduct in

2004 and 2005 and KFI's incurrence of almost a million dollars of attorneys' fees years later. Indeed, such fees are the classic example of "consequential damages," which may not be included in a restitution award. The district court's restitution award must therefore be vacated.

CONCLUSION

For the reasons stated, defendant Nosal should be acquitted on all six counts of conviction, or a new trial should be ordered on all six charges. Alternatively, the district court's restitution award should be vacated and remanded for reconsideration.

Dated: December 2, 2014

Respectfully Submitted,

DENNIS P. RIORDAN
DONALD M. HORGAN
RIORDAN & HORGAN

TED SAMPSELL JONES

By /s/ Dennis P. Riordan
Dennis P. Riordan

Attorney for Defendant-Appellant
DAVID NOSAL

STATEMENT OF RELATED CASES

Appellant is aware of no related cases pending in this Court.

CERTIFICATION REGARDING BRIEF FORM

I, Donald M. Horgan, hereby certify that the foregoing brief is proportionately spaced, has a typeface of 14 points, and contains 15,739 words as counted by the Word software program.

Dated: December 2, 2014

/s/ Donald M. Horgan
DONALD M. HORGAN

CERTIFICATE OF SERVICE
When All Case Participants are Registered for the
Appellate CM/ECF System

I hereby certify that on December 2, 2014, I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system.

I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

Signature: /s/ Jocilene Yue
Jocilene Yue

****
******

CERTIFICATE OF SERVICE
When Not All Case Participants are Registered for the
Appellate CM/ECF System

I hereby certify that on_____, I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system.

Participants in the case who are registered CM/ECF users will be served by the appellate CM/ECF system.

I further certify that some of the participants in the case are not registered CM/ECF users. I have mailed the foregoing document by First-Class Mail, postage prepaid, or have dispatched it to a third party commercial carrier for delivery within 3 calendar days to the following non-CM/ECF participants:

Signature: _____
Jocilene Yue