No. 16-10197

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

UNITED STATES,
Plaintiff-Appellee,

v.

MATTHEW KEYS,
Defendant-Appellant

Appeal from the United States District Court for the Eastern District of California
Criminal Case No. 2:13-CR-82 KJM (Hon. Kimberly J. Mueller)

APPELLANT'S REPLY BRIEF

Tor Ekeland
Mark H. Jaffe
TOR EKELAND, P.C.
43 West 43d Street, Suite 50
New York, NY 10036-7424
Tel: 718-737-7264
Fax: 718-504-5417
tor@torekeland.com
mark@torekeland.com

Jason S. Leiderman, SBN 203336
LAW OFFICES OF JAY LEIDERMAN
770 County Square Drive #101
Ventura, California 93003
Tel: 805-654-0200
Fax: 805-654-0280
jay@criminal-lawyer.me

Pro Bono Attorneys for Appellant Matthew Keys

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

OTHER AUTHORITIES

INTRODUCTION

A central issue in this appeal is the government's conflation of the unauthorized access prohibitions and unauthorized damage prohibitions of the Computer Fraud and Abuse Act ("CFAA"). The Superseding Indictment ("Indictment") charged felony unauthorized damage to a computer under the CFAA, as well as conspiracy and attempt to do so. Nowhere did it charge unauthorized access to a computer under the CFAA. Despite this, the government led its case and spent much of trial presenting evidence of uncharged conduct that went to proving unauthorized access under the CFAA. At times, the government argued at trial, and does so on appeal, that facts which constitute unauthorized access under the CFAA also constitute unauthorized damage. This is an incorrect and dangerous position, and would allow the government to turn an unauthorized access crime under the CFAA into a more harshly punishable unauthorized damage crime.

The government's interpretation would transform most of the CFAA's unauthorized access prohibitions into surplusage. In the court below, the government argued that actions typical of an unauthorized access crime constituted elements of unauthorized damage under the CFAA. For instance, the government argued that mere unauthorized possession of usernames and passwords threatened the "integrity" of the system and therefore constituted damage under 18 U.S.C. §

1030(a)(5)(A). Additionally, the government argued that copying data, an act common to unauthorized access cases, constituted CFAA damage. This conflation of the unauthorized access prohibitions of the CFAA with its unauthorized damage prohibitions is rife throughout the trial record.

This confusion and conflation of the two provisions contributed to the constructive amendment of the Indictment, the introduction of irrelevant and highly prejudicial evidence, and the improper consideration and conflation of CFAA damage and loss evidence at trial and at sentencing. Additionally, the government's arguments that Mr. Keys took a substantial step in his alleged attempt to cause damage to the Tribune Company's Content Management System ("CMS") fail. Mr. Keys' reconnaissance of the CMS is too attenuated from, and does not meet the *mens rea* requirements of, the elements of an unauthorized damage to a computer charge under the CFAA to constitute attempt. Therefore, this Court should reverse Mr. Keys' convictions on Count Two and Three of the Indictment. Finally, Mr. Keys' restitution should be vacated because it is based on speculative replacement costs.

ARGUMENT

I. THE GOVERNMENT CONSTRUCTIVELY AMENDED COUNT TWO OF THE INDICTMENT BY IMPROPERLY INTRODUCING UNCHARGED CONDUCT

The Government constructively amended the Indictment at trial through its repeated introduction and use of evidence, over objection, relating to uncharged conduct of Mr. Keys. This evidence related to the FOX40 television station in Sacramento, which had little to do with the edit of the LATimes.com website story on tax cuts (the "Edit") at issue in this prosecution. (*See* AOB at pp. 11-13.) The Indictment contains only one substantive charge, embodied in Count Two, which claims that the Edit was a felony violation of the CFAA. Count Two charges a violation of 18 U.S.C. § 1030(a)(5)(A), which prohibits "knowingly caus[ing] the transmission of a program, information, code, or command, and as a result of such conduct, intentionally caus[ing] damage without authorization, to a protected computer . . ."[1] 18 U.S.C. § 1030(a)(5)(A). Count One charged conspiracy under 18 U.S.C. § 371 to commit Count Two, and Count Three charged an attempt to violate 18 U.S.C. § 1030(a)(5)(A) by altering the front page of the Chicago Tribune.

[1] For the purposes of this Reply Brief, when referring to the language of 18 U.S.C. § 1030(a)(5)(A) stating that it requires transmission of a code, the use of the word "code" is meant to embody the entire "program, information…" statutory language. The differences between them are not at issue on this appeal.

Nothing in the Indictment indicates that the substantive charge should be read any way but to refer to alleged damage caused by the Edit. This is precisely how the District Court read the Indictment at the beginning of trial. (*See* SER 161 ("All of this said, I think the damage charged in the indictment is the damage to the L.A. Times website."). The government's repeated introduction, over the defense's repeated and standing objections, of evidence of the "Cancerman" email campaign and the copying of the FOX40 viewer promotion email address list ("Email Address List") led the District Court to express concerns that there was a variance.[2] Ultimately, this resulted in a constructive amendment of the Indictment.

There is no clear line between what constitutes a variance and what constitutes a constructive amendment. *See U.S. v. Ward*, 747 F.3d 1184, 1191 (9th Cir. 2014) ("The line that separates a constructive amendment from a variance is not always easy to define . . . ." (quoting *U.S. v. Adamson,* 291 F.3d 606, 615 (9th Cir.2002)); *see generally*, 3 Charles Alan Wright, Andrew D. Leipold, Peter J. Henning, Sarah N. Welling, *Fed. Prac. & Proc. Crim.* § 516 (4th ed. 2016) ("The distinction between variances and constructive amendments is a matter of degree, and the distinction is rather shadowy." (citations omitted)). A constructive amendment "typically mandates reversal," while "a variance requires reversal only

[2] The "Cancerman Emails" were a series of emails sent to FOX40 viewers and FOX40 employees complaining about FOX40 practices. (*See* AOB pp.11-12.)

if it prejudices a defendant's substantial rights." *Ward*, 747 F.3d at 1189 (quoting *U.S. v. Olson*, 925 F.2d 1170, 1175 (9th Cir.1991)).

Roughly speaking, a variance occurs when the proof at trial is materially different from the facts in the indictment, and a constructive amendment occurs when proof at trial changes the terms of the indictment. *See* 3 *Fed. Prac. & Proc. Crim.* § 516. This is a slippery distinction, made more elusive here by the government's pervasive use of facts related to Mr. Keys' FOX40 conduct. Those facts go toward proving unauthorized access to a FOX40 computer system, in contrast to the government's charge at trial of Mr. Keys' unauthorized damage to an LA Times computer system because of the Edit.

The CFAA, broadly speaking, prohibits two types of conduct. First, unauthorized access to a computer,[3] typified by 18 U.S.C. § 1030(a)(2)(C), prohibits unauthorized access to a computer and obtaining information. Second, in contrast, 18 U.S.C. § 1030(a)(5)(A) prohibits knowing transmission of a code, or the like, that intentionally causes damage to a computer. Under 1030(a)(5)(A), "Damage" is defined by the CFAA in 18 U.S.C.§ 1030(e)(8).

[3] This brief dispenses with the use of the phrase "protected computer" because it is not at issue here, and the definition is so broad that it is difficult to imagine any modern computer that would not be a "protected computer."

18 U.S.C. § 1030(a)(5)(A) does not require any unauthorized access, that is why it is routinely used to prosecute DDOS attacks.[4] A typical unauthorized access case involves accessing a computer, either through hacking a password or obtaining a password through improper means, and copying information. *See, e.g.*, *U.S. v. Nosal*, 676 F.3d 854, 856 (9th Cir. 2012) (reciting facts of CFAA prosecution for unauthorized access and downloading information); *U.S. v. Auernheimer*, 748 F.3d 525, 529 (3d Cir. 2014) (same). A typical 18 U.S.C. § 1030(a)(5)(A) prosecution involves the unauthorized destruction of data or rendering data inaccessible. *See, e.g. U.S. v. Shea*, 493 F.3d 1110, 1113 (9th Cir. 2007) (affirming conviction under §1030(a)(5)(A) for an employee's destruction of data). Generally, the baseline maximum sentence for an unauthorized access crime is five years. *See* 18 U.S.C. § 1030(c)(4) *et seq.* (listing CFAA penalties). The baseline maximum sentence for unauthorized damage under 18 U.S.C. § 1030(a)(5)(A), however, is ten years. *See* 18 U.S.C. § 1030(c)(4)(B)(i). There is a constructive amendment in this case, because, among other reasons, the prosecution blurred the distinction between these prohibitions, resulting in Mr.

[4] DDOS stands for "Distributed Denial of Service Attack. See *Denial-of-Service Attack*, available at https://en.wikipedia.org/wiki/Denial-of-service_attack (last accessed Jan. 30, 2016). 18 U.S.C. § 1030(a)(5)(B-C) requires unauthorized access that causes damage, but those provisions are not at issue here.

Keys being effectively charged with both unauthorized access and unauthorized damage.

The government's extensive use of Mr. Keys' FOX40 conduct put Mr. Keys on trial for unauthorized access in relation to FOX40, and not solely for damage to the LATimes.com caused by the Edit. (*See, e.g.* ER at 84, 120, 129-30.) Mr. Keys' unauthorized access to FOX40 content, the creation of new user accounts to access FOX40 content, and copying of the FOX40 viewer promotion email address subscriber list does not go to any element of damage to a protected computer under 18 U.S.C. § 1030(a)(5)(A). The cases that hold otherwise are bad law, as they would render the unauthorized access prohibitions of the CFAA surplusage. *See, e.g., NetApp, Inc., v. Nimble Storage, Inc.,* No. 13-CV-05158, 2015 WL 400251, at *11 (N.D. Ca. Jan. 29, 2015) (holding copying of data is not CFAA damage, rejecting the reasoning of courts that hold otherwise, and collecting cases); *Multiven, Inc. v. Cisco Systems, Inc.* 725 F.Supp. 2d 887, 894-95 (N.D. Ca. 2010) (holding that the "integrity of data" can be impaired by mere unauthorized possession of system passwords); *see also Williams v. Taylor*, 529 U.S. 362, 404 (2000) ("It is, however, a cardinal principle of statutory construction that we must 'give effect, if possible, to every clause and word of a statute.'"(citation omitted)). This confusion in the federal courts as to the meaning of "damage" under the

CFAA is at the forefront of this case, and underlies the constructive amendment of Count Two in the Indictment.

In an attempt to avoid the fact that its Indictment does not detail Mr. Keys' FOX40 conduct, and reads as if solely directed at damage to the LATimes.com CMS, the government attempts to style the Indictment as a general indictment that broadly encompasses all of Mr. Keys conduct prior to the Edit. (*See* Answer at 34.) The government maintains that when it superseded the original indictment by broadening its date range to include Mr. Keys' departure from FOX40 and his conduct before the Edit, it foreclosed any constructive amendment argument. (*See* Answer at 32-34.) However, the Indictment only expanded the date range of Count Two to include Mr. Keys' departure from FOX40, and added the general allegation that Mr. Keys "kept and used, for malicious purposes, login credentials to the Tribune Company's CMS. (Answer at 31-32 (citing ER 236-240 (Indictment)).[5] It did not mention the Cancerman emails, the exfiltration of the promotional subscriber email address list, the uncharged conduct of Sam Cohen's purported lock out of the CMS, or other facts relevant to the FOX40 conduct.[6]

[5] The government is correct when it points out that Appellant mistakenly stated in its opening brief that the only change to the Indictment was an expansion of the date range in Count Two. The government also added language saying Mr. Keys kept usernames and passwords for malicious purposes. This fact does not affect Appellant's arguments. (*See* Answer at pp. 31-32.)

[6] *See, e.g.,* AOB at 28.

The government was fully aware of these facts well before it superseded the original indictment. Indeed, its argument that the Indictment encompasses Mr. Keys' FOX40 conduct presupposes the government's awareness on this front. (*See* Answer at 33.) Yet none of that, with the exception of Mr. Keys' possession of login credentials that allowed him access to the LATimes.com website, is detailed in the Indictment.

The government's Answer does not cite any Ninth Circuit law on general indictments in relation to constructive amendment; it instead turns to other circuits. The cases it cites are distinguishable: in each, the conduct at issue was detailed in the indictment or went directly to the elements of the crimes charged. The government cites *United States v. Morgenstern*, 933 F.2d 1108, 1115 (2d Cir. 1991) for the proposition that "[w]here a generally framed indictment encompasses the specific legal theory or evidence used at trial, no constructive amendment occurs." (Answer at 33-34). But the Indictment here does not do so. It charged unauthorized damage to a computer, yet much of the trial was spent introducing evidence related to unauthorized access and other potential crimes such as harassment. *See, e.g.* 18 U.S.C. § 2261A (federal cyberstalking statute). The other Second and Fifth Circuit cases the government cites are distinguishable, as the evidence presented at trial in those cases went directly to the elements of the charges. *See U.S. v. Skelly*, 442 F.3d 94, 99 (2d Cir. 2006) (holding no constructive

amendment because the alternative theory of evidence applied to the charged securities and wire fraud conduct); *U.S. v. Salmonese* 352 F.3d 608, 621 (2d Cir. 2003) (holding that while conduct was not specifically pleaded in the indictment "[it was] plainly within the charged core of criminality . . . ."). Here, Mr. Keys' FOX40 conduct did not go to the core criminality as alleged in the Indictment. Thus, there was a constructive amendment.

A. The Court Should Review De Novo Because Mr. Keys Preserved His Constructive Amendment Objection at Trial

Mr. Keys sufficiently raised objections to the introduction of the FOX40 conduct multiple times on the record, including when arguing jury instructions, and thus de novo is the appropriate standard of review. *See, e.g, U.S. v. Hartz*, 458 F.3d 1011, 1019 (9th Cir. 2006); (AOB at 15, 18-20; ER at 126-127 (RT at 765-66); ER at 127 (RT 766:6-9); ER at 126 (RT 765:14- 17).) The District Court understood the Defense's objections and took them under advisement before jury charges were finalized.

In its Answer, the government argues that Mr. Keys' objections to the jury charges are insufficient to warrant de novo review, and that "[a]n objection to a jury instruction must be formal, timely, and distinctly stated." (Answer at 30.) But the *Ward* court declined to adopt this approach. *See U.S. v. Ward*, 747 F.3d at 1189 (9th Cir. 2014). Rather, the *Ward* court held that a defendant sufficiently preserved his objection by making the trial court generally aware of its concern of a possible

conviction based on uncharged conduct. *Id.* at 1189. The *Ward* Court held that the substance of defendant's objection, which stated that he was "worried" the jury would consider uncharged conduct, was "patently clear" even without mention of the Fifth Amendment, and de novo review was proper. *Id.*; *see also U.S. v. Lloyd*, 807 F.3d 1128, 1164 (9th Cir. 2015) ("The substance of Baker's objection was clear. Our review is de novo"). Thus, while the government argues that Mr. Keys should have made a pretrial submission of a "formal" and "distinctly stated" objection to the introduction of the FOX40 conduct, this Circuit's precedent prioritizes an objection's substance over form in the constructive amendment context.

Here, Mr. Keys requested that the District Court instruct the jury to ignore facts related to his FOX40 conduct and expressed concern to the Court that the Jury would be influenced to convict under Count Two due to the government's inclusion of uncharged conduct at trial. (ER at 126-27.) Because the Defense objected on multiple occasions to the introduction of the Cancer Man emails, and the substance of these objections were sufficiently clear to the trial court, de novo review is appropriate.

B. Even Under Plain Error Review, The Court Should Reverse Because a Constructive Amendment is Presumptively Prejudicial

Should this Court find that Mr. Keys' objections to the government's introduction of the FOX40 conduct are insufficient to warrant de novo review, this

Court should reverse under plain error review because the constructive amendment of the Indictment affected Mr. Keys' substantial rights by default. *See* Fed. R. Crim. P. 52 (requiring a finding of a substantial effect on a defendant's rights to warrant reversal).

In *U.S. v. Olano*, 507 U.S. 725, 735 (1993), the Supreme Court acknowledged that some errors are per se prejudicial, even when a defendant cannot demonstrate how an error affected their substantial rights. The Court held that, while a defendant must ordinarily prove that an error resulted in prejudice, some types of errors carry a presumption of prejudice. *Id.* at 735 ("Nor need we address those errors that should be presumed prejudicial if the defendant cannot make a specific showing of prejudice.)"

This Court has not yet found it necessary to definitively address whether a constructive amendment is presumed prejudicial under *Olano*. Sometimes it has found it unnecessary to reach *Olano*'s holding, as the defendant was, in fact, prejudiced by the constructive amendment. *See e.g., U.S. v. Dipentino*, 242 F.3d 1090, 1095 (9th Cir. 2001). Other times it has held that a "constitutional violation results" because a constructive amendment infringes a defendant's substantial right to be tried only on the indictment charges. *U.S. v. Alvarez-Ulloa*, 784 F.3d 558, 570 (9th Cir. 2015).

Various other circuit courts have adopted the *Olano* framework, applying this presumption in situations where defendants could not make a specific showing of prejudice. *See, e.g.*, *U.S. v. Reyna*, 358 F.3d 344, 351 (5th Cir. 2004) (presuming prejudice when a district court violated a defendant's rights of allocution); *U.S. v. Adams*, 252 F.3d 276, 286 (3d Cir. 2001) (same). Courts sitting in the Second, Third, and Fourth Circuits have held that in the context of plain error review, a constructive amendment of an indictment, by its very nature, affects a defendant's substantial rights and prejudice must be presumed. *See U.S. v. Syme*, 276 F.3d 131, 155 (3d Cir. 2002) (holding that that constructive amendment warrants a rebuttable presumption of prejudice); *U.S. v. Thomas*, 274 F.3d 655, 670 (2d Cir. 2001) (applying plain error review to constructive amendment and holding that the error is per se prejudicial); *U.S. v. Floresca*, 38 F.3d 706, 712 (4th Cir. 1994) (treating constructive amendments as a structural error that establishes per se prejudice). These courts held that a constructive amendment is per se prejudicial because it violates a basic right of all criminal defendants—the Fifth Amendment guarantee of a grand jury. *See Syme*, 276 F.3d at 154; *Floresca*, 38 F.3d at 712; T*homas*, 274 F.3d at 670. These courts have grounded the presumption in recognition of a defendant's right to have his jeopardy limited to offenses charged by a group of his fellow citizens. *See Floresca*, 38 F.3d at 712 ("There *should* be no question that the error affected Floresca's substantial right to grand jury indictment—after all, the

Supreme Court has already said that it does: a constructive amendment 'destroy[s] the defendant's *substantial right* to be tried only on charges presented in an indictment returned by a grand jury'" (internal citation omitted)).

If the Court holds that plain error review applies to the constructive amendment of Mr. Keys' Indictment, this Court should hold that it was per se prejudicial to Mr. Keys' substantial rights. Here, conduct left unarticulated in Mr. Keys' indictment was prominently featured at trial and repeatedly introduced and emphasized before the jury, including during opening and closing. (*See e.g.,* ER at 9-10, 55-56, 253.) In introducing this uncharged conduct to the jury, the government impinged on a core constitutional protection to prevent prosecutions "begun by arms of the Government without the consent of fellow citizens." *Thomas*, 274 F.3d at 670 (quoting *Stirone*, 361 U.S. at 217–19). The government unilaterally supplemented the Indictment with conduct that was not otherwise articulated by a grand jury as grounds for criminal charges under § 1030(a)(5)(A). This Court should presume that the constructive amendment prejudiced Mr. Keys, because the government encroached on Mr. Keys' right to have a grand jury of his peers first weigh and consider the evidence against him.

Additionally, this Court should adopt a presumption of prejudice, due to Mr. Keys' inherent difficulty in proving that details of his FOX40 conduct persuaded the Jury to find that the government established each element of Count Two. As

the Third Circuit has determined, a defendant's intrinsic hardship in proving whether a constructive amendment affected a verdict further supports the view that a presumption of prejudice should apply. *Syme*, 276 F.3d at 154. Because introducing this conduct integrally compromised the fairness and integrity of the judicial process, and because Mr. Keys cannot unequivocally prove that the Jury convicted on the basis of the Cancer Man emails, this Court should assume that the constructive amendment affected Mr. Keys' substantial rights.

II. THERE WAS NO ATTEMPT BECAUSE RECONAISSANCE OF THE CMS DID NOT CONSTITUTE A SUBSTANTIAL STEP TOWARDS ALTERING IT

Mr. Keys' cursory login attempt to the Chicago Tribune CMS does not constitute a substantial step towards causing damage to a computer. At best, it was an attempt at unauthorized access, conduct not charged in this case. The government cites *United States v. Nelson*, 66 F.3d 1036, 1042 (9th Cir. 1995) in its Answer for the proposition that "[a] substantial step is an 'appreciable fragment' of a crime, an action of 'such substantiality that, unless frustrated, the crime would have occurred." (Answer at 53.) But, under this standard, Mr. Keys' efforts to access the CMS do not qualify as a "substantial step." There are no other prior or subsequent acts in the record that relate to the alleged attempt, and Mr. Keys' hastily abandoned effort to log into the CMS does not constitute a substantial step to knowingly transmitting a code to intentionally cause damage to a computer.

Mr. Keys' spur of the moment effort to log in to the CMS was at best mere preparation. Mere preparation for a crime is insufficient to support an attempt charge. *See, e.g., Nelson*, 66 F.3d at 1042 (9th Cir. 1995) ("To constitute a substantial step, the defendant's actions must go beyond mere preparation, and must corroborate strongly the firmness of the defendant's criminal intent." (citation omitted)). In *U.S. v. Buffington*, 815 F.2d 1292 (9th Cir. 1987) the defendants did far more than Mr. Keys, and still did not pass beyond mere preparation. They assembled the materials to rob a bank, obtained weapons, and, while armed, left their parked car and stood with their attention focused on the bank. This took time, and presumably some foreknowledge as to the bank's location and hours. *See U.S. v. Buffington*, 815 F.2d at 1295 &1303. Despite this high level of preparation, this Court held that it was not enough to constitute "some appreciable fragment" of an attempted bank robbery. *Id.* Mr. Keys' preparation is far less than that of the *Buffington* defendants; where they stood armed in the parking lot outside, Mr. Keys, by analogy, slowed briefly outside the lot entrance before driving on.

The government also failed to meet its burden in proving the requisite specific intent to commit Count 3. In order to prove attempt, the government must prove that Mr. Keys had the specific intent to violate 1030(a)(5)(A) as well as the requisite intent the statute requires. *See U.S. v. Gracidas-Ulibarry*, 213 F.3d 1188, 1196-97 (9th Cir. 2000). Thus, the government was required to prove that Mr.

Keys had the specific intent to knowingly transmit a code with the specific intent to cause damage to a computer.[7] The proof at trial did not meet this burden.

Mr. Keys made a half-hearted attempt to log in to the CMS. He was not in possession of the mock-up of the front page at the time. There is nothing in the record that indicates he ever made a further attempt. And, even if Mr. Keys had the specific intent to commit damage to the CMS, his actions did not "unequivocally demonstrate" that the crime would have occurred unless interrupted by independent circumstances. *U.S. v. Still*, 850 F.2d 607, 609 (9th Cir. 1988). It is pure speculation to say what Mr. Keys would have done if he had accessed the CMS. Upon log in, he may have chosen to do nothing. At best his login attempt is an attempt at unauthorized access, but it is not sufficient for unauthorized damage.

III. THE PREPONDERANCE OF THE EVIDENCE DOES NOT SUPPORT THE RESTITUTION AWARD OF $249,956

The District Court's restitution figure is too arbitrary and too speculative to meet the preponderance of the evidence standard. The Tribune Company submitted no restitution figures in this case, yet the District Court ordered $249,956 in restitution. Out of this total, $200,000 was based on hearsay in an FBI 302 witness interview of Jerry Del Core, a FOX40 station manager. (*See* ER 163-64; Answer 57-58.)

The District Court arrived at the $200,000 restitution figure based on the "replacement cost" to build a new promotional database of viewers at $10 per "customer." (ER 164.) In its Answer, the government argues that replacement cost was the appropriate measure for calculating restitution. The government relies on *U.S. v. Kaplan,* 839 F.3d 795 (9th Cir. 2016) for this assertion, maintaining that this Court "recently approved use of replacement value as a basis to value an asset in restitution proceedings." The government, however, misapplies *Kaplan* and overstates its holding. The *Kaplan* court dealt with restitution for the loss of tangible, personal property.

In *Kaplan*, the district court ordered $40,000 of restitution for destroyed personal items that included clothing, furniture, and household appliances. *Id.* at 800. The district court calculated its restitution figure based on the replacement value of these tangible goods, as opposed to their fair market value, which would have reflected depreciation and would have been lower than their replacement value. *Id.* In affirming, the *Kaplan* court relied on other restitution case law that dealt with the loss of tangible, personal property. *See U.S. v. Frazier*, 651 F.3d 899, 908 (8th Cir. 2011) (remanding because district court did not make a factual finding as to a destroyed home); *U.S. v. Simmonds*, 235 F.3d 826, 829 (3d Cir. 2000) (calculating restitution for furniture damaged in a fire); *U.S. v. Shugart*,

176 F.3d 1373, 1376 (11th Cir. 1999) (affirming a district court's use of replacement value in determining the value of a burned-down church).

The facts in *Kaplan* are distinguishable from that of the instant case. Here, the government seeks restitution for the value of email addresses contained in an online database, not a tangible and largely fungible object. While the replacement cost measure in *Kaplan* is directly based on the ascertainable cost of replacing personal property, here no such value is apparent. Rather, the $10 per customer value is an arbitrary figure unsupported by either documentary evidence or expert testimony. Moreover, *Kaplan* discusses replacement value in a context in which personal property was no longer retrievable. Nothing in the instant case required replacement. The "customers'" email addresses were never deleted or damaged, but merely copied. FOX40 never lost any information in its viewer promotion database.

Moreover, a defined replacement value in this case is inappropriate because the government never established that the email addresses in the database were the "property" of Fox40. Beyond this, the government has not established how value of these email address lists should be measured. The government has failed to prove that the value of the database was customer participation in the contest, as opposed to the possession alone of email addresses for demographic or marketing purposes. Replacement value is thus the wrong metric to apply in this case, given

that the value of the email address list is not readily ascertainable and the value of the email address list has never been defined nor reliably determined with evidence.

The government seeks restitution for the Tribune Company's costs of generating an entirely new promotional list, in addition to the original promotional list that was copied and remains intact. The purpose of restitution under the MVRA, however, is to "make the victim[] whole" again by restoring to him or her the value of the losses suffered as a result of the defendant's crime. *U.S. v. Hunter*, 618 F.3d 1062, 1064 (9th Cir. 2010) (quoting *U.S. v. Crandall,* 525 F.3d 907, 916 (9th Cir.2008)). Here, the Tribune Company remained "whole" after Mr. Keys' uncharged conduct, unrelated to the Edit. Its promotional database was never deleted or damaged. Ordering restitution to pay for a new FOX40 promotional database is inconsistent with the purpose of the MVRA, as this would place the Tribune Company in a more advantageous position than it had been in prior to Mr. Keys' conduct. This could approximately double the amount of existing email addresses the Tribune Company has available for marketing purposes.

A calculation of restitution is limited to the victim's actual losses that are a directly and proximately produced by the defendant's offense. *U.S. v. Hunter*, 618 F.3d at 1064 (9th Cir. 2010). The government has failed to establish that Mr. Keys' conduct was a proximate cause of lost subscribers. The government has not

produced any evidence about the campaign's retention rate of customers prior to Mr. Keys' conduct, or how long the typical customer stayed on the list before unsubscribing. The government also failed to produce evidence concerning the quality of the subscriber campaign; another factor that would undoubtedly impact how long subscribers chose to stay. The government cites in its answer that it took "three years" to build the database back up to its prior level. (SER 997-98.) The government, however, fails to rule out that this three-year period could be attributable to other factors, such as a low quality or unattractive subscriber page, market effects, or declining use of mailing lists, all unrelated to Mr. Keys' conduct. Because there is no record on these or other variables, there is no reliable basis to prove that Mr. Keys' conduct was the direct or proximate cause of the campaign's lost subscribers.

IV. THE PREJUDICIAL EFFECT OF THE INTRODUCTION OF MR. KEYS' FOX40 CONDUCT FAR OUTWEIGHED ITS PROBATIVE VALUE

The District Court abused its discretion by allowing uncharged conduct of Mr. Keys in relation to FOX40 that occurred and ended before the Edit. The government cites a number of justifications for its admissibility, such as for proof of loss. None are availing, but the improper admission of loss evidence is the most prejudicial because felony liability under the CFAA in this case turns on it.

Loss under the CFAA must be causally related to the computer intrusion or impairment charged. *See, e.g., Farmers Ins. Exchange v. Steele Ins. Agency, Inc.* No. 13-CV-00784 2013 WL 3872950 at * 21) (E.D. Ca. July 25, 2013) ("To allege a loss under the CFAA, "plaintiffs must identify impairment of or damage to the computer system that was accessed without authorization.'" (citation omitted)); *Cassetica Software, Inc. v. Computer Scis. Corp.*, No. 09-CV- 0003, 2009 WL 1703015, at *4 (N.D. Ill. June 18, 2009) ("[T]o state claim based upon a loss, the alleged loss must relate to the investigation or repair of a computer system following a violation that caused impairment or unavailability of data . . . . Therefore, courts have found that costs that are not related to the impairment or damage to a computer or computer system are not cognizable 'losses' under the CFAA"). The CFAA's definition of loss has a reasonableness requirement, which invokes tort notions of direct and proximate causation. *See* 18 U.S.C. § 1030(e)(11) ("the term 'loss' means any reasonable cost . . . ."). In this case, any loss had to be causally related to the Edit on the LATimes.com website. That was the charged conduct in the Indictment, as Mr. Keys was not on trial for any alleged damage to FOX40. Thus, any loss evidence related to FOX40 was highly prejudicial, as it allowed the jury to use uncharged conduct to reach the $5000 threshold for felony liability under 18 U.S.C. § 1030(a)(5)(A) and its maximum

sentence of ten years of imprisonment. *See* 18 U.S.C. § 1030(c)(4)(A)(i); *Id.* at § 1030(c)(4)(B)(i).

The Cancer Man email campaign ended before the charged conduct in Count Two began. (Answer at 44.) Yet extensive testimony was admitted on the cost of responding to and investigating the Cancer Man email campaign. The same is true of the uncharged conduct involving Sam Cohen's alleged lock out from the FOX40 CMS. Neither event, distinct in time, caused the CFAA damage charged in this case. The only proper loss numbers permissible in this case are those caused by Mr. Keys' alleged Edit. Any others are too causally attenuated to support the heavy yoke of CFAA felony criminal liability and its attendant maximum ten-year sentence.

The government only cites civil cases to its implicit proposition that the Cancer Man emails, and Mr. Keys' uncharged FOX40 conduct, should be counted as loss resulting from damage under the CFAA. *Yoder & Frey Auctioneers, Incl v. EquipmenFacts, LLC*, 774 F.3d 1065 (6th Cir. 2014) is a civil case involving unauthorized access to a computer that recklessly caused damage. The loss, as described in the opinion, is a direct and causal result of the unauthorized access. *Id.* at 1072-73. *NovelPoster v. Javitch Canfield Group*, 140 F.Supp 3d 954 (N.D. Ca. 2014) is a decision on a motion to dismiss on two unauthorized access CFAA claims, one for unauthorized access and one for unauthorized access that recklessly

caused damage. *Novel* states that loss must be causally related to the CFAA violation. *NovelPoster* at 961("The upshot is that NovelPoster must show that defendants' violation of each of the alleged CFAA provisions caused loss . . . .").

Thus, the government is mistaken to argue that "the proper inquiry for the jury was what aggregate harm Keys caused" from his FOX40 conduct. (Answer at 33.) It cites *Creative Computing v. Getloaded.com LLC*, 386 F.3d 930, 935 (9th Cir. 2004) for the proposition that there is no single act requirement in the CFAA and that loss can be aggregated. This view, however, runs contrary to the fact that loss under the CFAA must be causally related to the computer impairment in question, as in *Creative Computing*. *See id.*; *Nexans Wires S.A. v. Sark-USA, Inc.*, 166 Fed. Appx. 559, 562 (2d Cir. 2006); 18 U.S.C. § 1030(e)(11). The Indictment here charges impairment damage to the LATimes.com from the Edit, not any damage to FOX40 (including the purported lockout of Sam Cohen). Loss may be aggregated when it is causally related to the charged computer impairment, but aggregation of loss is not proper for causally unrelated conduct. None of the cases cited by the government stand for the proposition that felony liability may be imposed in a CFAA case on the basis of aggregated CFAA loss attributed to uncharged conduct. Indeed, our research reveals no case that says this. Therefore, the District Court abused its discretion in allowing evidence of Mr. Keys' FOX40 conduct because it

was highly prejudicial when it came to reaching the $5000 threshold for felony liability under 18 U.S.C. § 1030(a)(5)(A).

V. THE RULE OF LENITY IS OF IMPORT BECAUSE THE CFAA IS GRIEVOUSLY AMBIGUOUS AND UNCERTAIN IN BOTH LANGUAGE AND STRUCTURE

The government is incorrect to say the Rule of Lenity "has no import" here. (Answer at 49.) The government quotes this Court's decision in *U.S. v. Wanland*, 830 F.3d 947, 953-54 (9th Cir. 2016) for the proposition that "[t]he rule of lenity only applies . . . where there is grievous ambiguity or uncertainty in the language and structure of the statute, such that even after a court has seized everything from which aid can be derived, it is still left with an ambiguous statute." This describes the CFAA perfectly. The CFAA is a statute of "grievous ambiguity or uncertainty" both "in language and structure." The myriad of conflicting interpretations nationally as to what constitutes unauthorized access, unauthorized damage, or loss proves this.

Currently, as this Court knows, there is a circuit split over the meaning of unauthorized access. *See, e.g. U.S. v. Nosal*, 676 F.3d 854, 862 (9th Cir. 2012) (discussing circuit split); *U.S. v. Valle*, 807 F.3d 508, 523 (2d Cir. 2015) (discussing the problem of defining the scope of exceeding authorized access and noting "[o]ver the past fourteen years, six other circuits have wrestled with the question before us."); Orin S. Kerr, *Vagueness Challenges to the Computer Fraud*

and Abuse Act, 94 Minn. L. Rev. 1561 (May 2010). There also is confusion as to the meaning and scope of CFAA damage across the country. *See, e.g., Multiven, Inc. v. Cisco Systems, Inc.* 725 F.Supp. 887, 894 (N.D. Ca. 2010) (holding that mere unauthorized possession of a username and password constitutes CFAA damage); *NetApp, Inc. v. Nimble Storage, Inc.*, No. 13-CV-05058, 2015 WL 400251, at *11 (N.D. Cal. Jan. 29, 2015) (holding the mere copying of data is not CFAA damage but noting disagreement among district courts). What counts as CFAA loss in one jurisdiction does not in another. *S. Parts & Eng'g Co., LLC v. Air Compressor Servs., LLC*, No. 1:13-CV-2231-TWT, 2014 WL 667958, at *5 (N.D. Ga. Feb. 20, 2014) (acknowledging the presence of a district court split).

This interpretative black hole is highly problematic given that an individual can traverse multiple jurisdictions over the internet at the speed of light. In short, there is no dearth of cases interpreting the CFAA's language in different ways. To add fuel to the fire, the government's interpretation of the meaning of CFAA damage would render its structure grievously ambiguous and uncertain.

The government cites the legislative history of the oft amended CFAA for the proposition that CFAA damage includes "systems users changing their passwords" and "system administrators [having] to devote resources to re-securing the system." (Answer at 49 (citing Sen. Rep. No. 104-357, at 11 (1996).) But, as

discussed above, if this is CFAA damage then the distinction between the unauthorized access and unauthorized damage prohibitions embodied in the CFAA is largely extinguished. Almost every instance of unauthorized access involves system users having to change their passwords and system administrators having to devote time to re-securing the system. This is to say nothing of the fact that most unauthorized access cases involve the copying of information, which, if copying constitutes CFAA damage, means that it is also a case of unauthorized damage. This overbroad reading of the CFAA is particularly dangerous in the criminal context, as it can mean the difference between a maximum sentence of five years and ten. *See* Above, Part I.

Given the Rule of Lenity, and the CFAA's grievous ambiguity and vagueness both in language and structure (if the government's argument is to be credited), this Court should limit the CFAA definition of damage to the deletion of data for which there is no back up, or where access to data is significantly impaired. (*See* AOB at 35-37.)

CONCLUSION

The government's conflation of the CFAA's unauthorized access and unauthorized damage prohibitions led to a constructive amendment in this case. The government introduced voluminous evidence of uncharged conduct, proof of unauthorized access to a computer but not unauthorized damage. This, in effect,

added an additional charge to the Indictment, constructively amending it. Thus, Count Two should be reversed. As for Count Three, the government's proof was insufficient to prove that Mr. Keys took a substantial step to alter the Chicago Tribune CMS when he acted with little preparation and his cursory login attempt to the CMS was nothing more than a form of reconnoitering. Therefore, Count Three should be reversed. Finally, the restitution judgment against Mr. Keys should be vacated because, among other reasons, it is based on speculative replacement costs for information that was neither deleted nor the property of FOX40, and thus fails to meet the preponderance of the evidence standard.

Dated: January 30, 2017

Respectfully Submitted,

By: */s/Tor Ekeland*

Tor Ekeland
Mark H. Jaffe
TOR EKELAND, P.C.
43 West 43d Street, Suite 50
New York, NY 10036
Tel: 718-737-7264
Fax: 718-504-5417
tor@torekeland.com
mark@torekeland.com

Jason S. Leiderman, SBN 203336
LAW OFFICES OF JAY LEIDERMAN

5740 Ralston Street, Suite 300
Ventura, California 93003
Tel: 805-654-0200
Fax: 805-654-0280
jay@criminal-lawyer.me

Pro Bono Attorneys for
Defendant Matthew Keys

CERTIFICATE OF SERVICE

I hereby certify that on January 30, 2017, I electronically filed the foregoing with the Clerk of the Court for the U.S. 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.

By: */s/Tor Ekeland*

Tor Ekeland
TOR EKELAND, P.C.
43 West 43rd Street
Suite 50
New York, NY 10036
Brooklyn, NY 11201
Tel: 718-737-7264
Fax: 718-504-5417
tor@torekeland.com

Jason S. Leiderman, SBN 203336
LAW OFFICES OF JAY LEIDERMAN
5740 Ralston Street, Suite 300
Ventura, California 93003
Tel: 805-654-0200
Fax: 805-654-0280
jay@criminal-lawyer.me
Pro Bono Attorneys for Defendant Matthew Keys

Certificate of Compliance with Rule 32

Certificate of Compliance With Type-Volume Limitation, Typeface Requirements, and Type Style Requirements

1. This brief contains 6,506 words, excluding the parts of the brief exempted by Fed. R. App P. 32(a)(7)(B)(iii).

2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Word for Mac Version 15.24 in 14 point Times New Roman font.

Dated: January 30, 2017

By: */s/Tor Ekeland*

Tor Ekeland

TOR EKELAND, P.C.
43 West 43rd Street
Suite 50
New York, NY
10036
Tel: 718-737-7264
Fax: 718-504-5417
tor@torekeland.com

Jason S. Leiderman, SBN 203336
LAW OFFICES OF JAY LEIDERMAN
770 County Square Drive, Suite 101

Ventura, California 93003
Tel: 805-654-0200
Fax: 805-654-0280
jay@criminal-lawyer.me

Pro Bono Attorneys for Defendant-Appellant Matthew Keys