COURT OF APPEAL OF THE STATE OF CALIFORNIA

FOURTH APPELLATE DISTRICT, DIVISION ONE

PEOPLE OF THE STATE OF CALIFORNIA, Plaintiff and Respondent, v. KEVIN CHRISTOPHER BOLLAERT, Defendant and Appellant.	CASE NO. D067863 SAN DIEGO COUNTY SUPERIOR COURT NO. SCD252338

APPEAL FROM THE SUPERIOR COURT OF SAN DIEGO COUNTY

(HONORABLE DAVID M. GILL, JUDGE)

APPELLANT'S OPENING BRIEF

Patrick J. Hennessey, Jr.
Attorney At Law (047993)
2356 Moore Street, Suite 201
San Diego, CA 92110
(619) 298-7802
Attorney for Appellant

By Appointment of the Court of Appeal Under the Appellate Defenders Independent Case System.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Rules

COURT OF APPEAL OF THE STATE OF CALIFORNIA

FOURTH APPELLATE DISTRICT, DIVISION ONE

PEOPLE OF THE STATE OF CALIFORNIA, Plaintiff and Respondent, v. KEVIN CHRISTOPHER BOLLAERT, Defendant and Appellant.	CASE NO. D067863 SAN DIEGO COUNTY SUPERIOR COURT NO. SCD252338

APPEAL FROM THE SUPERIOR COURT OF SAN DIEGO COUNTY

(HONORABLE DAVID M. GILL, JUDGE)

APPELLANT'S OPENING BRIEF

STATEMENT OF APPEALABILITY

This appeal is from a final judgment following trial by jury and is authorized by Penal Code section 1237.

STATEMENT OF THE CASE

In amended information filed on January 13, 2015, appellant, Kevin Bollaert, was charged in count one with conspiracy to commit identity theft in violation of Penal Code sections 182, subdivision (a)(1) and 530.5. Counts 2, 4, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 21, 23, 24, 26, 27-30, 32, 35 charged appellant with identify theft in violation of Penal Code section 530.5, subdivision (a). Counts 3, 5, 6, 20, 22, 25, 31, 33-34, 36, charged appellant with extortion in violation of Penal Code section 520. (1CT 164-176.)

During the course of trial, counts 4, 5, 9, 10, 34-36 were dismissed either on appellant's motion pursuant to Penal Code section 1118.1 or the People's motion to dismiss. (CT 167-175.)

Following trial, the jury was deadlocked as to counts 1, the conspiracy, and 25. The court declared a mistrial as to both counts. Appellant was found guilty of the remaining counts. (3CT 724-772.) On April 3, 2015, appellant was sentenced on count 3 the middle term of three years. A two-year midterm was imposed on count two but stayed pursuant to Penal Code section 654. Consecutive 8-month (one-third of the midterm) terms were

imposed on counts 4-15, 17, 19, 20, 22-26 and 28. Consecutive one-year terms (one-third of the midterm) were imposed on counts 16, 18, 21, 27, and 29. The total county prison term was 18 years. Appellant was given credit for 124 days of presentence custody. The court imposed a $10,000 restitution fine and a $10,000 probation/parole revocation fine. The court ordered a $1,080 court operations assessment, a $154 criminal justice administrative assessment and a $10 criminal conviction assessment. Also ordered was $15,489.88 in restitution to the victims. (3CT 773-777.)

Notice of appeal was filed April 13, 2015. (CT 646.)

STATEMENT OF FACTS

A. Introduction.

In 2012-2013 appellant and another individual set up a website "Yougotposted." The site would post photos, often nude, of both men and women. The photos and information as to the individual's state and/or city of residence, Facebook page and/or other social media addresses were provided by third parties, in most cases people having had prior relationships with the persons whose photos were posted.

The website also provided a link wherein those whose photos were posted could request they be removed. In some cases the photos were removed for free and in others individuals paid a fee to have the photos removed from the website. The link for removal of the photos used by most of the individuals was "changemyreputation.com." Following an investigation by officials of the California Department of Justice, appellant, Kevin Bollaert, took down the website and was cooperative with investigating agents as to their inquires regarding his actions relating to the website.

B. People's Witnesses.[1]

Brianna-Count 6

In October of 2013 Brianna discovered that photographs of her had been posted on a website. She received this information from comments on her Facebook account. She searched the website and saw a number of her pictures, including nude pictures, had been posted on the website, "Yougotposted." (4RT pp. 267-270.) Brianna believed that the photographs had been taken by a former boyfriend who also may have been behind a number of harassing messages she received following posting of the photographs. (4RT pp. 275-276.)

Brianna described how she received a number of unsolicited emails that were offensive to her. (4RT p. 272.) Brianna stated that she paid no money to have the pictures removed from the site. (4RT p. 276.)

[1] A number of the individuals whose photos were posted testified and generally provided the same information as to their discovery that their photos had been posted, information as to who provided the photos to the website as well as a discussion of the distress and/or other issues arising from the posting of the photos. A summary as to each witness will be provided.

Alice-Count 11

In August of 2013, Alice had gone to a party. She believes that someone put a drug in a cocktail she consumed. Two to three days later, she found photos of her posted on the website. She also received a number of salacious messages from strangers about the photos. (4RT pp. 277-278.) Alice was not sure who took the photos but a male identified in one of the photos was a friend of a friend of hers. The posting stated where she lived and other information such as a Facebook site. Alice contacted Yougotposted and asked that the photos be removed. She received a response stating that there was a charge to pay in order to have the photos removed from the site. (4RT pp. 281-283.) Alice did acknowledge that the photos were probably taken by a friend of hers, Joey and his girlfriend. She did not pay any money to have the photos removed. (4RT pp. 284-286.)

Nicole C.-Count 14

In May of 2014, Nicole C. received a number of lewd messages on her Facebook account. Most of these were from strangers. She later discovered that her photos had been posted on the website. She had taken the photos for her ex-fiancée who apparently sent the photos to the

website. (4RT pp. 290-293, 295.) The photos caused Alice to be very upset. She dropped out of school and had difficulty obtaining a job. She did not pay any money to the website. (4RT pp. 293-295.)

Alaina-Counts 21-22

In May of 2013, Alaina received a call at her place of employment from someone who had told her that her photos had been posted on the website. (4RT p. 296.) She sent a number of emails to Yougotposted asking the photos be taken down. She then contacted the site Changemyreputation and made a $350 payment. The photos were removed the following day. The photos and the fact that other people had seen them caused her to become upset. (4RT pp. 298-303.)

Jocelyn-Count 27

Jocelyn described that in the same time period she had pictures posted on Yougotposted. She received word from a friend of her sister that her photos were there. The fact the photos were posted caused her issues at home and at work. She also received a number of vulgar contacts from various strangers. (4RT pp. 308-312.) Jocelyn noted that she may have told investigators the

pictures were taken down from the site within two days of a call from her sister. (4RT p. 314.)

Megan-Count 17

In January of 2013 Megan took a number of "selfies", some of which were nude photos. She in turn sent the photos to her boyfriend and one other person. She later learned the photos had been posted on the website as she began receiving messages from strangers. She requested the photos be taken down and nothing happened. She was concerned because the website listed her name and her hometown. Megan believed that the photos were submitted to the website by someone she knows and that appellant was not responsible for that. (4RT pp. 318-327.)

Ashley-Count 28

In July of 2013, Ashley received word that her photos had been posted on the website. She received a number of messages from strangers as to the photos. She also stated that many people in her hometown knew about the posting. Ashley stated the photos were taken for her boyfriend but she did not know if he was the one who posted them on the website. She contacted "Yougotposted" and asked that the photos be removed but to her knowledge they were not taken down. (4RT pp. 330-333.)

Kristina-Count 26

Kristina recalled that in July 2013 nude photographs of her were posted on the website. Also posted was information as to her town of residence and her Facebook account. She received a number of vulgar messages from people she did not know. Kristina noted that the photos had been sent by her to a man she was dating. She noted that one of her boyfriends to whom the photos were sent wanted more nude photos of her before he would ask that the site remove the photos down. (4RT pp. 339-346.)

Brittany-Count 16

In July of 2013, Brittany received information from friends that photos of her had been posted on the website. She received a number of messages from strangers that she found humiliating. She went to the site and viewed the photos. She recognized them as photos sent to a boyfriend who had been deployed overseas with the military. Brittany made several requests to have the photos removed. (4RT pp. 349-356.) She was unsure whether it was the boyfriend who sent the photos to the website. (RT 357.)

Nina-Count 12

In mid-August of 2013 a number of nude photos of Nina were posted on the website. The posting listed her name and the city in which she lived as well as her Facebook page. She believed the boyfriend posted the photos on the website. (4RT pp. 399-400, 404.) She received a number of vulgar messages from strangers and contacted the website to have the photos removed. The link to "changemyreputation" asked for a $500 payment to remove the photos from the website. (4RT pp. 404-405.) She also noted that the same photos had been sent to another website "myEx.com" that was unrelated to appellant. (5RT p. 412.)

Sarah-Count 15

In May of 2013, a number of photos of Sarah were posted on the website. She received this information from friends on Facebook. The site provided her full name and the city in which she lived. As a result she received a number of derogatory comments from strangers. (5RT pp. 537-539.) Sarah requested the photos be deleted on two separate occasions. At one point the photos were removed and then reposted, including new photos. She believed that it was possible some party unrelated to

appellant may have hacked into her email account. (5RT pp. 542-546.)

Barbara-Count 23

In June of 2013 Barbara received word that a number of her photos had been posted on the internet. The photos had been taken and were intended for her husband. She tried to have them removed and received a response that a payment was required to remove the photos. (5RT pp. 552-562.)

Jasmine-Counts 32-35

In June of 2013 a number of Jasmine's photographs were posted on the website. Also included was her name as well as her social media contact information. It created difficulty at her work when they found out about the photos. The photos were originally intended for her boyfriend who was the individual responsible for posting them on the website. Jasmine paid $500 to have the photos removed. (5RT pp. 582-586.)

Jennifer-Counts 19-20

In late 2012 and early 2013 a number of photographs of Jennifer were posted on the website. She received a number of comments from individuals that she did not know as to the posting. She asked the site to remove them.

She paid $249.99 to "changemyreputation" to have the photos removed. (5RT pp. 595-600.)

Jane Doe-Count 7

In May of 2013, Jane began receiving messages from strangers regarding a posting on the internet. She located a number of her photos that had been posted on the site. This posting caused her problems at her school as well as her work. She contacted an attorney who in turn contacted the website. Ultimately the photos were removed after the contact by her attorney. She believed an ex-boyfriend had posted her photos on appellant's website as well as another site unrelated to appellant. (5RT pp. 605-617.)

Rebecca-Counts 2-3

In March of 2013 Rebecca received calls from her manager and others on her Facebook account regarding a posting. The photos were of her and an ex-fiancée. (6RT pp. 627-629.) She recalled sending an email to both "Yougotposted" and "changemyreputation" requesting the photos be removed. She was requested through the site "changemyreputation" to make a PayPal payment for $249.99 to have the photos removed. The photos were removed within minutes of the payment. (6RT pp. 633-637.) She

noted it was her ex-boyfriend who posted the photos and he was also the individual who contacted her manager at work. (6RT p. 640.)

Christina-Count 18

In the middle of 2013 Christina had a number of photographs posted on the website. She believes the photos were posted by someone who had stolen her cell phone. The listing gave her name and city of residence as well as her Facebook address. Posting of the photos caused issues with her family. Christina noted that she had a third party contact "Yougotposted" to have the photos removed. She did not receive a reply. (6RT pp. 644-647.)

Emily-no count alleged[2]

In June of 2013 photographs Emily had sent to her fiancée were posted on the website. She believes it was her ex-fiancée who posted the photos. She attempted to have the photos removed but was unsuccessful. She noted that one of the links requested a payment to have the photos taken down. (6RT pp. 659-665.)

---

[2] The court allowed limited testimony for a number of parties who were not included in counts in the amended information.

Kaye-Count 13

In August of 2013 a number of Kaye's photographs were posted on the website. The site listed her name, hometown, as well as her Facebook and Twitter accounts. She received a number of derogatory comments regarding the postings. Kaye contacted the police who sent an email to "Yougotposted" advising them she was a juvenile. She acknowledged the photos had been sent to a friend in 2010 and suspects he may have been the one who posted them. (6RT pp. 678-686, 689.)

Manuel-Counts 29-30

Manuel related that a number of his photos had been posted on the website and he believed they had been sent by a friend of his. Manuel made a payment of $250 to "changemyreputation" to have the photos removed. (6RT pp. 692-695.)

Brian-Counts 24-25

In March and April of 2013 Brian had a number of his photographs posted on the website. Also included were his name and hometown plus his Facebook page. Brian paid $250 to have the photos removed. (6RT pp. 706-715.)

Aurora-Count 1

Aurora had a number of photos posted in September of 2013. She became aware of the posting when she received several Facebook messages related to the posting. She did not pay any money but noted that the site shut down several weeks later. (6RT pp. 724-731.)

Ms. V-Count 8

In June of 2013, Ms. V testified she had a number of photos that she had sent to an ex-boyfriend posted on the "Yougotposted" website. She received a number of messages from people she did not know regarding those pictures. (6RT pp. 771-772.) Ms. V noted that the photos were taken down one week later and that she made no payment to have them removed. (6RT pp. 775-777.)

As to some of the above-noted victims, a stipulation was entered into between the parties clarifying certain aspects of their testimony. As to victim Ashley it was stipulated that the person seeking additional nude photos of her was not appellant. It was also stipulated as to Barbara that "changemyreputation.com" did not interact with the public through any live chat or phone calls. Additionally, the site requesting $5,000 from her to remove the photos was not appellant's. As to Sarah it

was stipulated that she told The Attorney General's investigator, Daniel Torres, that she had sent the photos to her ex-boyfriend plus ten other people. Finally, it was stipulated as to Jocelyn that she had told investigator Torres that the photos had been removed within two days and never reposted. (8RT pp. 1045-1046.)

Mark Kelly operates a forensic accounting firm that works on occasion for the California Department of Justice. (5RT p. 373.) He has access to a number of programs by which he can search information from data stores on other devices (computers). In April of 2014 he was asked by the Department of Justice to obtain forensic images from appellant's computers. (5RT pp. 374-380.) Kelly was able to determine appellant was using an HP laptop. The main computer was described as HPDV7. (5RT p. 385.)

By further examination Kelly was able to determine there were list of names including most of the victims on that particular computer. Kelly believed appellant was in control of that computer. (5RT pp. 386, 395.) He believed appellant was the administrator of the website who reviewed the contents before posting. (5RT pp. 396, 412.) Kelly was also able to determine that a number of

payments had been made to the "changemyreputation.com" website, also administered by appellant. (5RT p. 428.) Kelly noted that the "changemyreputation" site was set up by appellant and that it would be readily observable on the "Yougotposted" site to refer people for payment. (5RT p. 439.) The site set up by appellant and which Kelly believed he maintained generally required an email address, a name, and a location by city and state of anyone posting on the website. The site also asked for, but did not demand, Facebook information. (5RT p. 453.)

As best Kelly could tell, that computer was last used in September of 2013. This generally coincided with the time in which he believed the site was shut down. (5RT p. 460.) Kelly was able to identify 119 payments made to the websites. (5RT p. 465.) Kelly made no claim appellant created the content but did believe appellant was able to edit the contents of the pages in his administering the website. (5RT pp. 488-489.) Kelly noted that "Yougotposted" was an example of a website that offered public opportunities to share or read text and photos. (5RT p. 502.) Kelly also noted the site specifically limited terms of usage to people over the age of 18. (RT 507.)

Agent Brian Cardwell of the California Department of Justice electronic crimes unit was asked to look into the "Yougotposted" case in July of 2013. (6RT pp. 778-779.) At that time the site was still active and appellant was the registered owner of the site. Agent Cardwell obtained the search warrant for the server on the site seeking information as to "yougotposted." (6RT pp. 782-787.)

Cardwell ultimately meet with appellant in San Diego on September 18, 2013. At that time they spoke for approximately 50 minutes in an interview that was recorded. (Court's Exhibit 1.) (6RT p. 790.) On that September 18 date Cardwell took possession of appellant's laptop, a full size HP laptop, an Ipad and a Macintosh. (6RT pp. 817-818.)

Agent Cardwell believed that there had been over 10,000 postings on the website and that there were approximately 2,500 requests seeking removal of information posted on that site. (6RT pp. 817-818, 7RT p. 841.)

Cardwell noted that in their interview appellant stated that all content was submitted by third parties. He merely supplied a "billboard" for others to use.

Cardwell acknowledged that there are other similar sites in existence. The site ultimately closed in September of 2013. (7RT pp. 844-846.)

Michelle Moreno an auditor with the Department of Justice examined PayPal documents related to appellant's website. She determined in excess of $30,000 had been paid by various people through appellant's PayPal account. (7RT pp. 884-894.)

ARGUMENT I

APPELLANT'S CONVICTIONS FOR IDENTITY THEFT UNDER PENAL CODE SECTION 530.5(a) MUST BE SET ASIDE AS HE WAS NOT AN INFORMATION OR INTERNET CONTENT PROVIDER AND THEREFORE COULD NOT BE PROSECUTED UNDER THAT STATUTE.

A. Introduction.

The People proceeded on three separate theories as to why appellant fell within the purview of Penal Code section 530.5(a), identity theft. They proceeded, and the jury was instructed that there were three separate theories upon which the People were proceeding: (1) violation of Penal Code section 653(m); (2) public disclosure of private facts; and (3) intrusion into a person's private affairs. (2CT 385-388.)

Penal Code section 530.5 specifically provides that interactive service providers and access software providers, as defined by the Communications Decency Act (47 U.S.C. section 230, shall not be held liable absent a showing of fraud. Penal Code section 530.5(f) provides:

> An interactive computer service or access software provider as defined in subsection (f) of section 230 of Title 47 of the United States Code (the Communications Decency Act) shall not be liable under this section unless the service provider acquires, transfers, sells, conveys, or retains possession of personal information with the intent to defraud.

Appellant's convictions for identity theft cannot stand because no identity theft occurred and his conduct was protected by the Federal statue which supersedes laws of the State of California.

B. The Law.

The standard of appellate review on the question of sufficiency of the evidence to support a verdict was stated in *People v. Towler* (1982) 31 Cal. 3d 105, 117-119:

> "The recent cases of *Jackson v. Virginia* (1979) 443 U.S. 307 [61 L.Ed.2d 560, 99 S.Ct. 2781] and *People v. Johnson* (1980) 26 Cal. 3d 557 [162 Cal.Rprt. 431, 606 P.2d 738], refine the standard of review which governs our consideration of the sufficiency of the evidence contention on this appeal. In *Jackson*, the United States Supreme Court held that 'the critical inquiry on review of the sufficiency of evidence to support a criminal conviction [is] to determine whether the record evidence could reasonably support a finding of guilty beyond a reasonable doubt.' (443 U.S. at p. 318 [61 L.Ed.2d at p. 573].) The *Jackson* court went on to explain that 'this inquiry does not require a court to ask whether it believes that the evidence at the trial established guilt beyond a reasonable doubt.' [Citation] Instead the relevant question is whether, after reviewing the evidence in the light most favorable to the prosecution, any rational trier of fact could have found the essential elements of the crime beyond a reasonable doubt.' (*Id.* at pp. 318-319 [61 L.Ed.2d at p. 573].)
>
> "In *Johnson*, our court found California's traditional sufficiency of the evidence standard of review consistent with *Jackson*, emphasizing that in passing upon such a claim 'a court must review the

> whole record in the light most favorable to the judgment below to determine whether it discloses substantial evidence – that is, evidence which is reasonable, credible and of solid value – such that a reasonable trier of fact could find the defendant guilty beyond a reasonable doubt.'" (26 Cal.3d at p. 578.)
>
> The court in *Towler* later noted:
>
> "Whether the evidence presented at trial is direct or circumstantial, under *Jackson* and *Johnson* the relevant inquiry on appeal remains whether any reasonable trier of fact could have found the defendant guilty beyond a reasonable doubt. (See, e.g. *People v. Cordova* (1979) 97 Cal.App.3d 665, 669–670; *People v. Young* (1981) 120 Cal.App. 3d 683, 693–694.)" (*Id.* at p. 118.)

On review the appellate court must view the record in a light most favorable to the People, as the party which prevailed below and draw reasonable inferences from the evidence presented to the trial court in support of its judgment. (See, *People v. Marshall* (1997) 15 Cal.4th 1, 34; *People v. Vann* (1974) 12 Cal.3d 220, 225.) However, in *People v. Johnson*, *supra*, 26 Cal.3d 557, it was noted that while an appellate court must view the evidence in a light most favorable to the respondent and presume in support of the judgment the existence of every fact a trier could reasonably deduce from the evidence, this review is not limited only to evidence favorable to the respondent. The question as to the sufficiency of the evidence must be judged in light of the entire record

and whether the evidence on each essential element is substantial. It is not enough for respondent to simply point to some evidence supporting the finding. (*Id.* at pp. 576–577.)

A defendant's convictions based upon insufficient evidence where no reasonable trier of fact should have found defendant guilty of the charged offenses violates his rights to due process under the United States Constitution. (See *Jackson v. Virginia* (1979) 433 U.S. 307, 318 [61 L.Ed.2d 560, 99 S.Ct. 2761].) The evidence in appellant's case fails to establish he violated any California statute and further, his actions were protected by The Communications Decency Act (CDA), the controlling federal statute. While the record is generally reviewed in a light most favorable to the judgment below, the evidence in appellant's case to be reviewed by this court does not support the verdicts. (*Id.* at p. 318 [61 L.Ed.2d at p. 573].)

C. Discussion.

The Internet is one of the most diverse forums for individual communication ever invented. In its short life the Internet has moved from the province of technical specialists and educational institutions into a

powerful force in the everyday lives of most Americans, allowing them to share, discuss, and develop ideas in their political, professional, and personal lives. As the U.S. Supreme Court observed 15 years ago, "It is no exaggeration to conclude that the content on the Internet is as diverse as human thought." (*Reno v. American Civil Liberties Union* (1997) 521 U.S. 844, 852.) Not surprisingly, the scope and depth of legal protections for Internet service providers played a direct role in whether and how speech will develop on line.

1. Communications Decency Act.

In 1996, Congress passed section 230 of the Communications Decency Act ("CDA 230") or ("Section 230") taking a deliberate, affirmative step to protect speech online by broadly shielding Internet service providers from responsibility for materials supplied by their users. Congress recognized that immunizing interactive computer services from liability for hosting diverse content in turn encourages the development and availability of innovative online services that foster free speech. Because it encourages both large and small intermediaries to open forums for discussion, section 230

has been critical in protecting and expanding the Internet as a forum for free speech.

The Communications Decency Act of 1996 provides:

> "No provider or user of an interactive computer service shall be treated as a publisher or speaker of any information provided by another information content provider." (47 U.S.C. section 230, subdivision (c)(1).)

The Communications Decency Act was enacted by Congress specifically to prevent actions against internet service providers that would constitute intrusive regulation on free speech. (*Zeran v. America Online, Inc.* (4th Cir.1997) 129 F.3d 327, 330.) The law specifically forbids actions against interactive computer services and access software providers based on content they displayed that was created by or originated by third parties. The law does not prevent states from enforcing criminal statutes consistent with the statute. (47 U.S.C. section 230, subdivision (e)(3).) Nor does it prevent enforcement of federal criminal statutes. The Act does preclude enforcement of state actions that are inconsistent. (Subdivision (e)(1), (3).)

In this case, the People seek to chip away at the clear protections provided by the Communications Decency Act. The People claim the statute's protection did not

apply to Yougotposted because Yougotposted administered the website and possessed the authority to pick and choose which information was posted. Here the People's reliance on speculation and conjecture fails to strip appellant of the statute's immunity. If the People's arguments are accepted, the approach would provide an avenue for other litigants to end-run the bright-line protections provided by the statute, jeopardizing service providers and undermining speech in the process. This amounts to bad policy.

2. Penal Code section 530.5.

Penal Code section 530.5, subdivision (f) provides:

> "An interactive computer service or access software provider as defined in subsection (f) of Section 230 of Title 47 of the United States Code (The Communications Decency Act) shall not be liable under this section unless the service or provider acquires, transfer, sells, conveys or retains possession of personal information with the intent to defraud."

As a result, absent an intent to defraud, appellant, an internet service provider and access software provider, cannot be held liable under Section 530.5.

3. Appellant is not Liable Under Penal Code Section 530.5 Because he is (1) an Interactive Computer Service Provider and (2) an Access Software Provider as Defined in the Communications Decency Act and There was no Fraud.

In appellant's case the People produced no evidence supporting their belated claim that appellant possessed any personal information with the intent to defraud. California jury instructions describe fraud as having deceived another person in order to cause a loss of money or something of value or damages to a legal, financial or property right. (See CALCRIM 2041.) The People's belated claim that the payments he obtained through "changemyreputation.com" were obtained by fraud because the victims were unaware appellant owned both websites. There are two problems with this argument made below. First, the link to "changemyreputation.com" was published on "yougotposted.com." There was no attempt or evidence suggesting appellant was hiding that the sites were connected. For example, victim "Alaina" testified that to her it was "obvious" that the same person was behind both sites. (4RT pp. 305-306.) Additionally, who the victims believed the payment was going to is of no significance. They were paying to have the pictures removed, not because they were "deceived". There was simply no deception in this case.

Under The Communications Decency Act, a party is immune from liability if they are an interactive computer

or service provider or an access software provider. The act defines "interactive computer service provider as any information service, system or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions." (*Id.* at subdivision (f)(2).) An access software provider "is defined as, a provider of software (including client or server software, or enabling tools that do any one or more of the following: (A) filter, screen, allow or disallow contents; (B) pick, choose, analyze or digest contents; or (C) transmit, receive, display, forward, cache, search, organize, reorganize, or translate content." (Subdivision (f)(4).) The evidence presented at trial established appellant was an interactive computer service provider as well as an access software provider. The site he established performed all of the functions described above.

The protections of the Communications Decency Act immunized providers of "interactive computer services" and their users from causes of action asserted by persons

alleging harm caused by content supplied by others. (See *Fair Housing Counsel of San Fernando Valley v. Roomates.com, LLC* (9th Cir. 2008) 521 F.3d 1157, 1179.) There the court noted:

> [CDA 230] provides a safe haven for interactive computer service providers by removing them from the traditional liabilities attached to speakers and publishers. (*Id.*, citing *Zeran v. America Online, Inc.*, *supra*, 129 F.3d 327, 330.)

Information content providers do not receive immunity under the CDA. They are defined as "any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service." (Subdivision (f)(3).) The People argued below that appellant was an information content provider because he received the images submitted by third parties and elected whether or not to post them to the website. This was not disputed at trial. However, the courts have consistently held that engaging in this type of a selection process does not render a party an "information content provider." It is well settled that operators of websites and providers of interactive computer services such as appellant are not information content providers.

(See *Universal Communications Systems Inc. v. Lycos, Inc.* (1st Cir. 2007) 478 F.3d 413, 419.)

The Fourth Circuit has made it clear that a lawsuit seeking to hold the service provider liable for its exercise of a publisher's traditional editorial functions-such as deciding whether to publish, withdraw, postpone or alter content-are barred. (*Zeran v. America Online Inc.*, *supra*, at p. 330.)

In *Zeran*, a third party made numerous posts to an *America Online* message board falsely suggesting that the plaintiff, Mr. *Zeran*, was selling t-shirts and other merchandise celebrating the bombing of the Oaklahoma City Federal Court Building. The post included *Zeran*'s home phone number and resulted in *Zeran* receiving abusive phone calls which threatened him with violence and death. These calls were often received as little as two minutes apart. *America Online* was specifically put on notice about the postings and they declined to remove them. (*Id.* at p. 329.)

It was held America Online was not liable under The Communications Decency Act even though they were put on notice about the contents of the posts and deliberately took no action to remove them from the message board

system they had operated. The court held that actively deciding to leave the third-party content on the website was a publishing decision and did not change their status as an interactive service provider.

Similarly, in *Batzel v. Smith* (9th Cir.2003) 33 F.3d 1018, the operator of a listing service/on line bulletin board selected and posted a letter that had been submitted by a third party stating that an attorney in Northern California bragged that she was the granddaughter of Adolf Hitler's "right hand man" Heinrich Himmler, and because of this the attorney possessed many valuable stolen paintings which rightfully belonged to people who died in the Holocaust. The Ninth Circuit specifically analyzed whether the operator of a list service became a content provider as opposed to an interactive service provider by screening, editing and selecting the letter submitted by a third party. The court noted:

> The pertinent question becomes whether Smith was the sole content provider, or whether Cremars (the website operator) can also be considered to have 'created' or 'developed' Smith's email message forwarded to the listserve…Cremars did not create Smith's email… Nor did Cremars' minor alterations to Smith's email prior to its posting or his choice to publish the email (while rejecting other emails for inclusion in the listserve) rise to the level of 'development.'" (*Id.* at p. 1031.)

In 2009, the Ninth Circuit noted in *Barnes v. Yahoo! Inc*. (9th Cir. 2009) 570 F.3d 1096, 1102, that "reviewing, editing and deciding whether to publish or withdraw from publication third party content" does not render a party a content provider and outside the scope of The Communications Decency Act. In *Barnes*, an unhappy former boyfriend of the plaintiff created a profile for her on Yahoo! wherein he posted nude pictures, taken without her permission, and posted open solicitations for sex. He also posted her real and electronic addresses as well as the phone number for her place of employment. She was then inundated with disturbing, harassing contacts from strangers. Yahoo! was specifically and repeatedly put on notice and never took any action to remove the offensive material. The court found the refusal to remove material was well within the scope of The Communications Decency Act. The court cited its earlier decision in *Batzel* noting that, "it is immaterial whether this… comes in the form of deciding what to publish in the first place or what to remove among the published material." (*Batzel*, *supra*, 333 F.3d at p. 1032.)

In *Calofano v. Metrosplash.com Inc.* (9th Cir.2003) 339 F.3d 1119, the court addressed the question of whether a website becomes a content provider when they require third party users to answer specific questions in order to use the site. In that case a third party created a profile on an internet dating site for a woman without her permission. The third party posted pictures of the woman that were readily available on line. The third party filled out statistical information required by the website and additionally posted the woman's home address as well as her email address and telephone number. The third party then wrote and posted open ended statements suggesting the woman sought to be sexually dominated and suggested she was promiscuous. She then received a number of frightening and explicit contacts from strangers. The Ninth Circuit specifically rejected the contention the dating website was a content provider because it required users to answer prepopulated questions. While the questionnaire on the website facilitated expression of information by individual users, the selection of the content was less exclusively to the user. (*Id.* at p. 1124.) As in appellant's case there is nothing inherently wrong with asking for this

information. Simply asking for statistical information is not actionable.

More recently, in *Jones v. Dirty World Entertainment Recordings, LLC* (6th Cir.2014) 755 F.3d 398, a website known as "TheDirty.com" allowed people to post disparaging and defamatory pictures, videos and comments about other people. In this particular case "TheDirty" was sued by a woman who was both a high school teacher and a cheerleader for the Cincinnati Bengals National Football League team. "TheDirty" chose to post submissions by third parties suggesting she had engaged in sex acts with the entire football team and that she had numerous sexually transmitted diseases. The post even went so far as to specify the high school where she taught. All of this subjected her to unwanted contacts, shame, ridicule and disgrace.

Initially, the U. S. District Court found the Communications Decency Act did not apply. The court reasoned that the website by its nature had intentionally encouraged and invited actionable third party postings and therefore took part in developing content. However, the Sixth Circuit overruled the lower court's finding and found that the Communications Decency Act did apply. The

court held that the lower court was wrong in finding "TheDirty" was an information content provider because it had encouraged actionable third party postings. The court stated that "an encouragement test would inflate the meaning of 'development' to the point of eclipsing the immunity from the publisher liability that Congress established." (*Id.* at p. 414.)

The court held "TheDirty" could not be deemed an information content provider. The fact the website encouraged and solicited actionable material, the fact that the website's operator ratified and adopted the actionable material by adding his own commentary did not make the website operator a content provider. It was also noteworthy that in this case the court noted that the "TheDirty" required third party users to submit a title and category for their submissions which included a location by naming either a city or college. The third party user was specifically instructed by the website to specify "who, what, when, where, why." (*Id.* at p. 403.)

The plain text of CDA 230 makes clear that Congress created this immunity to limit the impact of Federal or State regulation imposed on the Internet either through statute or through the application of common law causes

of action. (See, e.g., 47 U.S.C. Section 230, subdivision (a)(4).) The Internet and other interactive computer services "have flourished, to the benefit of all Americans, with a minimum of Government regulation"; (*Id.* section 230, subdivision (b)(2)) "[i]t is the policy of the United States" to minimize Internet regulation). This policy of regulatory forbearance squarely applies to any liability imposed based on the exercise of traditional editorial functions such as to publish or withdraw third party content. Such liability was, "for Congress, simply another form of intrusive Government regulation of speech." (*Zeran*, *supra*, 129 F.3d at 330.) Congress thus recognized in section 230 what the U.S. Supreme Court later confirmed in extending the highest level of First Amendment protection to the Internet:

> "governmental regulation of the content of speech is more likely to interfere with the free exchange of ideas then to encourage it." (*Reno*, *supra*, 521 U.S. at p. 885, see also *Batzel v. Smith*, *supra*, 333 F.3d at p. 1027, ("Congress wanted to encourage the unfettered and unregulated development of free speech on the Internet, and to promote the development of the E-commerce.").

The Communication Decency Act (CDA 230) itself provides:

> "it is the policy of the United States … to encourage the development of technologies which maximize user control over what information is

> received by individuals, families and schools who use the Internet and other interactive computer services." And "to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation." (47 U.S.C. Section 230, subdivision (b)(2), (3).)

Congress is concerned that imposing liability on providers who host thousands or even millions of messages might lead to overreaching moderation or outright censorship is even more pressing today. When the Communications Decency Act was passed approximately 40 million people used the Internet worldwide. Commercial online services in the United States at that time had almost 12 million individual subscribers. (*Reno*, *supra*, 521 U.S. at p. 850.) Today the number of worldwide internet users exceeds two billion. (International Telecommunication Union [UN Agency for information and communications technology], issue 5 (January, 2011).) The difficulties related to policing third party content has grown exponentially along with the number of people now regularly speaking online.

By its plain language, section 230 creates a federal immunity to any cause of action that would make a service provider liable for information originating with third-party user of the service. (*Zeran*, *supra*, 129 F.3d at p.

330.) The courts have consistently applied its immunity broadly, not sparingly, to encourage free speech on the Internet. (See, e.g. *Nemet Chevrolet, Ltd., v. Consumeraffairs.com, Inc.* (4th Cir.2009) 591 F.3d 250, 254.) CDA 230 clearly precludes any cause of action brought against a person under any state or local law that is inconsistent with the section. (See *Carofano v. Metrosplash.com, Inc.* (9th Cir. 2003) 339 F.3d 1119, 1125.)

Based on the above and based on evidence produced at trial appellant is an interactive computer service provider who took no action that amounted to developing or creating the content. Appellant's convictions of identity theft are in direct conflict with the first amendment and the Communications Decency Act. Both the Communications Decency Act and Penal Code 530.5(f) specifically immunize him from prosecution.

4. The Evidence Presented at Trial Fails to Establish Appellant's Guilt for Identify Theft Not Protected by the Communications Decency Act.

There was also some argument below that appellant was guilty of identity theft because he willfully obtained someone else's personal identifying information and used that information for an unlawful purpose and

that the person used the information without the consent of the person whose identifying information he was using. This contention is not sustainable.

The evidence does not support the conclusion appellant willfully obtained any personal identifying information of the alleged victims. Willful implies simply a willingness to commit the act, or to make the omission referred to. It does not require any intent to violate the law, or injure another, or to acquire any advantage. The court *In Re Rolando S.* (2011) 197 Cal.App. 4th 936 addressed the question of willfully obtaining the identifying information of another. In *Rolando S.* the victim had used his ex-girlfriend's Facebook password to access her personal Facebook page and post obscene messages and comments purporting to be the victim herself.

The court found that by receiving a text message from the victim wherein she gave him the password and choosing to save/remember that password the defendant had willfully obtained the password. In appellant's case the third parties who submitted the material, ex-boyfriends etc. and/or personal enemies, who posted the personal information on the website would be akin to the defendant

in *Rolando S*. Appellant's position is not the same. Appellant only provided the opportunity for third parties to post the information of their choice. The statutes have not been used to prosecute a website host operator for felonies or for crimes based on the actions of a third party. The People's argument below wrongly suggests the law should be extended to criminalize the business practice of merely hosting a website.

Aside from much speculation, the People's argument was that appellant exercised his editorial discretion regarding the placement of information that was allegedly personal identifying information of another person to be used for an unlawful purpose. No such unlawful purpose has been established on this record. The protections under Section 230 apply categorically and without any inquiry into the motivations of the provider and regardless of the provider's motive or mental state in making his editorial decisions. (See e.g. *Green v. America Online* (3d Cir.2003) 318 F.3d 465, 470-471.)

It is also interesting to note that Penal Code section 647, subdivision (j)(4) has been recently enacted to provide:

> Every person who commits any of the following acts is guilty of a misdemeanor:...Any person who

> photographs or records by any means the intimate body parts or parts of another identifiable person, under circumstances where the parties agree or understand that the image shall remain private, and the person subsequently distributes the image taken, with the intent to cause serious injury or emotional distress, and the depicted person suffers serious emotional distress.

This law addresses people such as the defendant in *Rolando S.* and the third parties who posted the photos to appellant's website. Nothing in this statute suggests applicability to individuals engaged in the business of operating the website. Appellant's conduct simply does not constitute identity theft within the meaning of the statute.

5. Appellant Did Not Use the Identifying Information for an Unlawful Purpose.

There was some suggestion below that appellant used the personal identifying information for the unlawful purpose of fraud or harassment in violation of Penal Code section 653(m) or for the purpose of committing the civil tort of "invasions of privacy".

Penal Code section 653, subdivision (m), provides:

> Every person who, with intent to annoy, telephones or makes contact by means of electronic communication device with another and addresses to or about the other person any obscene language . . .is guilty of a misdemeanor.

In appellant's case there was absolutely no evidence appellant contacted any of the alleged victims. He directed no obscene language to them. All these acts were undertaken by third parties unknown to appellant. Section 653 applies to third parties who seek out the website of their own free will, then decide to take down the information on the website and make the additional decision to direct obscene messages to particular individuals. Here, there was absolutely no contact by the website operator, appellant. The evidence does not support appellant's use of the identifying information for an unlawful purpose.

Similarly, appellant did not use the personal identifying information for the purpose of invading the victim's privacy or any fraudulent purpose. Under California law the tort of invasions of privacy requires:

> (1) the plaintiff had a reasonable expectation of privacy in specific information.
>
> (2) the defendant intentionally intruded into that matter.
>
> (3) the defendant's intrusion would be highly offensive to a reasonable person.
>
> (4) the plaintiff was harmed.
>
> (5) the defendant's contact was a substantial factor in causing the harm.

In deciding whether the plaintiff had a reasonable expectation of privacy in a particular act, the tort requires consideration of:

(1) the identity of the defendant.

(2) the extent to which other persons had access to or could see or hear the plaintiff.

(3) the means by which the intrusion occurred.

(See CACI 1800).

As noted above, the unlawful purpose as to invasion of privacy may be attributed to the third parties who submitted the photographs to appellant's website, but not to appellant. Appellant did not know any of the alleged victims. Third parties sought out his website and chose to use it to post the photos without permission. These third parties acted of their own free will. In fact, appellant could not tell from the submissions whether the people submitting the photos were submitting photos of themselves or other people without their permission.

Another question is whether it was established each of the victims had a reasonable expectation of privacy in the photos. Most, if not all of the alleged victims admitted they knowingly took or allowed to be taken the photos which they then in turn shared with other people. It has been noted that transmissions over the Internet

are not reasonably expected to be private. (See *United States v. Lifshitz* (2d Cir. 2004) 369 F.3d 173; *Four Navy Seals v. Associated Press* (2005) 413 F.Sup. 1136, 1143.) In this case there was no evidence the victims retained their right to the images once they willingly distributed them over the Internet or gave them to third parties.

Under any of the above theories the People's case must fail. The evidence fails to establish appellant falls outside the protections of The Communications Decency Act or that the identifying information was posted for any unlawful purpose not otherwise protected.

There in no "good faith" requirement written into the blanket protections of 47 U.S.C. Section 230, subdivisions (c)(1). Such a requirement would be antithetical to the broad protections provided by the statute. Any use of the information provided by third parties is not actionable as to appellant. As an interactive service provider appellant falls squarely within the statute's protections.

ARGUMENT II

THE EVIDENCE FAILS TO SUPPORT APPELLANT'S CONVICTIONS FOR EXTORTION.

A. Introduction.

The People argued that appellant used the posting of the photographs on the website to illegally obtain money from those whose photos were posted and to have the photos removed from the "Yougotposted" website. The People argued that appellant threatened to injure the victims or "expose their secrets" by publishing the images on the website. As the CDA provides, interactive computer service providers and access software providers are under no legal obligation to remove postings submitted to their website by third parties, even those postings that are negative in nature. Appellant was simply under no obligation to remove the negative content from his website. He merely offered a service to remove the photos and, by offering such a service, he is engaging in standard business practice and not extortion.

B. The Law.

In general, to be guilty of the crime of extortion a person must (1) threaten to unlawfully injury another person or threaten to expose a secret about another person or to expose them to disgrace and (2) when making

the threat, the defendant intended to use the fear engendered by that threat to obtain the person's consent to give the defendant money and (3) as a result of the threat the other person gave the defendant money. (Penal Code sections 519, 520.)

In order to establish extortion, the wrongful use of force or fear must be the operating or controlling cause compelling the victim's consent to surrender the thing to the extortionist. (See *Chan v. Lund* (2010) 188 Cal.App. 4th 1159, 1171.) The "secret" referred to in the extortion statute is the matter unknown to the general public, or to some particular part thereof which might be interested in obtaining knowledge of the secret. The secret must concern some matter of fact relating to things past, present or future and must affect the threatened person in some way so unfavorable to the reputation or to some other interest of the threatened person that the threatened exposure would likely to induce a person through fear to pay money or property for the purpose of avoiding the exposure. (*Cross v. Cooper* (2011) 197 Cal.App. 4th 357, 386, 387.)

C. Discussion.

Penal Code section 519 describes fear used to extort and enumerates threats to:

1. Do an unlawful injury to the person or property of the individual threatened or of a third person.

2. To accuse the individual threatened or any relative of his, or member of his family, of any crime.

3. To expose, or to impute to him or them any deformity, disgrace or crime, and

4. To expose any secret affecting him or them.

In this case the People proceeded on the theory that the third-party postings constituted exposure of a secret affecting the persons portrayed in the photos. The initial reaction is that appellant's operation of the website and posting information provided solely by third parties simply does not constitute a threat to expose any secret as to the other persons because the alleged secret (photos) was already in the public domain and had been provided by third parties unaccompanied by any demand for payment. In this case there is absolutely no evidence any request was made through either "Yougotposted" or "changemyreputation.com" before the photos had been submitted by the third parties. In this case appellant

merely provided a means whereby, for a fee, information already legally posted could be removed.

The question of extortion as it relates to Internet service providers was recently discussed in *Levitt v. Yelp!, Inc.* (9th Cir. 9/2/14) __ F.3d ___. The court found that Yelp!, Inc., a website that allows the public to post reviews of businesses, was not engaging in extortion by calling business and asking them to pay for advertising in exchange for more positive reviews, fewer negative reviews and overall higher ratings. In *Yelp!*, business owners claimed they often received less than favorable reviews from customers that were posted on Yelp! *T*hey would be then contacted by representatives of Yelp! who asked them to pay for advertising with implied assurances that the result would be more positive reviews, fewer negative reviews and/or the listing of reviews in such an order as to place the more favorable reviews at the top.

In *Yelp!*, several of the businesses claimed that if the solicitation for advertising was rejected, Yelp! immediately would remove positive reviews and elevate the negative reviews. It was also alleged that Yelp! was fabricating negative reviews that made disparaging and

untrue claims about the businesses. It was also alleged Yelp! manipulated the rating system to give the non-advertising companies poor ratings. Numerous business owners claimed that the Yelp! practice was for sales representatives to advise them that if they decided to pay for advertising they would help hide the negative reviews and adjust the rating to favor the business.

The Ninth Circuit discussed the Hobbs Act (a civil extortion statute) and California Penal Code sections 519 and 520, concluding that the statutes are virtually the same. The court concluded that Yelp!, as an internet service provider, was not engaging in extortion. The court noted:

> In sum, to state a claim of economic extortion under both Federal and California law, the litigant must demonstrate either that he had a pre-existing right to be free from the threatened harm, or that the defendant had no right to seek payment for the service offered. Any less stringent standard would transform a wide variety of legally acceptable business dealings into extortion.

The court found the plaintiffs had no pre-existing right to a positive review and that Yelp! was in no way obligated to refrain from manipulating reviews or creating negative ones. Yelp! was simply offering a service when it offered to remove negative reviews from its web page and that the offering of that service in

exchange for money amounted to a legitimate business practice. (*Id.*)

In the present case, appellant, as an interactive computer service provider was under no legal obligation to remove the postings submitted to the website by third parties, even when those postings are negative in nature. As in the above cited cases, *Yelp!*, *Yahoo!*, *AOL* and the dating website in the *Carofano* case, as well as "TheDirty.com" case, appellant could legally decline to remove any offending content from his website. Offering a fast, efficient removal service through the site "changemyreputation.com" amounted to a legal practice, akin to the practices approved in *Yelp!*. No crime of extortion occurred. Yelp! offered to remove negative content for money. They were under no obligation to remove those negative reviews and they offered the additional service in exchange for a fee. This is a business practice, not extortion.

Extortion is a specific intent crime. (*People v. Hesslink* (1985) 167 Cal.App. 3d 781, 788.) To sustain a conviction for extortion the People must have proved that the defendant acted with the specific intent to:

(1) threaten to unlawfully injure another person; or threaten to expose a secret about another person; or to expose them to disgrace.

(2) when making the threat the defendant intended to use fear to obtain the person's consent to give them the money, and

(3) as a result of the threat the other person gave the defendant money. (CALCRIM 1830.)

In this case there was no evidence that appellant threatened to expose a secret or disgrace of any alleged victim. First, appellant never threatened the alleged victim and, second, there could be no threat to expose a secret or disgrace when that very secret or disgrace has already been exposed to the world. In this case there is no threat and therefore no extortion. Appellant's only interaction with those whose photos were posted was initiated by those people who requested he provide the additional service of removing their photos from the website. No threats were made, either direct or implied. Appellant never sought out or contacted any of the victims. He took no affirmative action by word nor did he "threaten".

Finally, extortion convictions cannot be upheld where the alleged secret or disgrace has already been exposed. Under the Penal Code the extortionist must threaten to expose a secret or disgrace. This would

impliedly mean that the secret or disgrace would be at some future time exposed unless the extortionist is paid a sum to keep that secret unexposed. In the present case it was undisputed the alleged victims received no prior notice, warning or threat that the pictures were going to be posted on any website. In fact, virtually all had put the photos over the internet by their own act of sending them to ex-boyfriends or others. When the victims were notified of the posting on appellant's website, the images had already been accessible to anyone with a computer and the inclination to check out the website.

These acts, under the plain meaning of the statute, did not constitute extortion. It has been held that information publicly available on websites "to any one interested in knowing about it" does not constitute a secret for purposes of extortion. (*Cross v. Cooper* (2011) 197 Cal.App. 4th 357, 387-388.) In *Cross*, tenants emailed their landlord and threatened to tell prospective purchasers of the property that a registered sex offender lived nearby if the landlord did not agree to allow them to live rent free for a month. The Court of Appeal found that as a matter of law, this could not constitute a threat to expose a secret for the purpose of extortion

because the information that the offender lived in the neighborhood is publicly available on the website to anyone who is interested in knowing about it. (*Id.* at p. 387.) As in appellant's case, the images were already publicly available to anyone interested in knowing about them.

The plain language of the statute and the case law demonstrates appellant did not threaten to expose any secret or disgrace within the meaning of the statute. The fact that he advertised a conduit through which already-exposed information could be removed does not support any charge of extortion. As in *Yelp!*, it is a business practice that is plainly not extortion when there has been no threat to expose a secret or disgrace already exposed.

ARGUMENT III

THE TRIAL COURT ERRED IN INSTRUCTING THE JURY WITH CACI CIVIL LITIGATION INSTRUCTIONS THAT ALLOWED THE JURY TO ELEVATE A POSSIBLE CIVIL WRONG INTO AN ELEMENT OF THE CRIMINAL OFFENSE OF UNAUTHORIZED USE OF PERSONAL IDENTIFYING INFORMATION BASED ON PENAL CODE SECTION 653m, SUBDIVISION (a).

A. Introduction.

The trial court instructed the jury that an unlawful purpose required for the unauthorized use of personal identifying information as charged in various counts could be shown based upon a violation of Penal Code section 653m, subdivision (a). In relation to this theory, the court instructed the jury, pursuant to the People's request, with CACI 1800 and 1801, intrusion into private affairs and public disclosure of private facts, respectively. (2CT pp. 387-388.) In each case the instruction was prefaced with the following statement by the court:

> An unlawful purpose required for the unauthorized use of personal identifying information as charged in several counts ___ may also be based upon a claim of invasion of privacy by . . . .

The court then, as to each, instructed that the finding could be based on private affairs or public disclosure of private facts. (2CT 387-388.)

Each of the requested CACI instructions was based upon civil liability and actions arising from obligations under civil law. The trial court effectively elevated these alleged possible civil wrongs into an unlawful (criminal) purpose to become crucial elements of Penal Code section 653m(a). In turn, these "elements" of the crime could be found based on a civil law theory and establish the use of personal identifying information for "an unlawful" purpose. Appellant believes giving both of these instructions was error as the standard applied to a civil wrong is lower than beyond a reasonable doubt as is applied to a criminal offense and all elements of that offense. Here the trial court wrongly allowed the use of some civil wrong to be elevated by the jury into a criminal wrong-an unlawful purpose. The error was prejudicial, particularly in light of the inability to determine whether jurors relied on this theory in support of their convictions for the identity theft counts.

B. The Law.

It is well settled that the trial court functions as both a neutral arbiter between two contesting parties and the jury's guide to the law. This requires the court instruct the jury on the law applicable to each issue.

It is also settled that in a criminal case, even in the absence of a request, the court must instruct the jury on the general principles of law relevant to the issues raised by the evidence. The general principles are those closely and openly connected to the facts before the jury and which are necessary for the jury's understanding of the case. (*People v. Sedeno* (1974) 10 Cal.3d 703, 715-716; *People v. St. Martin* (1970) 1 Cal.3d, 524, 531.)

In general, a determination of whether there is sufficient evidence to support a particular instruction is a question of law and subject to independent review. (*People v. Barnett* (1998) 17 Cal.4th 1044, 1045.) The instructional errors are viewed *de novo* and without deference. (*People v. Waidlaw* (2000) 22 Cal.4th 690, 733; *People v. Shaw* (2002) 97 Cal.App. 4th 833, 838.) In this case the trial court gave instructions which substantially lowered the People's burden of proof by allowing them to elevate what may or may not have been some type of civil liability into a crucial element of a criminal offense finding. It so infused a trial with unfairness as to deny appellant his right to due process. (*Estelle v. Maguire* (1991) 502 U.S. 62, 75.)

C. Discussion.

It is well established that there is a substantial difference between civil and criminal cases. Each has a different burden of proof. In a criminal case, the prosecution has the burden of proving each element of the charged crime beyond a reasonable doubt. (*People v. Cole* (2004) 33 Cal.4th 1158, 1208.) In order to overcome the presumption of innocence, the prosecution must prove the defendant guilty beyond a reasonable doubt.

It is error for the trial court to give any instruction to the jury in a criminal case that shifts the burden of proof to the defendant. (See *People v. Banks* (1976) 67 Cal.App. 3d 379, 383-384; *Mullaney v. Wilbur* (1975) 421 U.S. 684, 704 [95 S. Court 1881, 1892].) The current instructions given by the court were based on their applicability to civil cases. In such cases private parties are suing one another, usually seeking monetary damages. The attendant burden of proof is much less stringent. For example, in a civil lawsuit involving self-defense or the defense of another, the defense of self-defense in response to a claim of assault is what is generally referred to as an "affirmative defense." As an affirmative defense, it is the

defendant's burden to prove facts supporting the affirmative defense by a preponderance of the evidence. (See *Bartosh v. Banning* (1967) 251 Cal.App. 3d 378, 386.)

In this case the court instructed the jury that they could use either intrusion into private affairs as described under civil law or public disclosure of private facts also as described in civil law to be the equivalent of an unlawful (criminal) purpose required to establish elements of the crime of identity theft. Both of these theories were strongly argued by the People to support the identity theft counts. As noted, had appellant been engaged in the conduct described in either CACI 1800 or 1801, the result might have been some undetermined civil liability, but not criminal liability. This is without any discussion of protected actions under the CDA. The use of elements of civil wrongs to establish criminal liability was error.

The People must show beyond a reasonable doubt that the erroneous instructions did not impact the result. (*Chapman v. California* (1967) 386 U.S. 18; see also *People v. Flood* (1999) 18 Cal.4th 470, 502-503.) *Chapman* holds that a violation of most federal constitutional rights requires reversal unless the prosecution can

establish beyond a reasonable doubt that the violation did not affect the result. Under this standard the question becomes whether there exists a reasonable possibility a more favorable outcome would have resulted absent the error.

Even under the standard of *People v. Watson* (1956) 46 Cal.2d 818, the error here was prejudicial. After examination of the entire record, it is reasonably probable appellant would have obtained a more favorable outcome as to the identity theft counts had the jury been properly instructed. Reasonably probable does not mean appellant must establish that it is more likely than not the error affected the outcome of the case. Rather, probable in this context does not mean more than a 50% chance but merely a reasonable chance, more than an abstract possibility. (*College Hospital Inc. v. Superior Court*(1994) 8 Cal.4th 704, 715.) At a minimum, appellant has established that the probabilities of prejudice and harmlessness are equally balanced and under *Watson* this establishes a miscarriage of justice has occurred. (*Id.* at p. 837.)

CONCLUSION

For the foregoing reasons, appellant requests that his convictions be reversed.

Respectfully submitted,

/s/Patrick J. Hennessey, Jr.
PATRICK J. HENNESSEY, JR.

CERTIFICATION OF WORD COUNT

People v. Bollaert

I, Patrick J. Hennessey, Jr., hereby certify that according to the computer program used to prepare this document, Appellant's Opening Brief contains 10,900 words.

I declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct. Executed this 23d of October, 2015, in San Diego, California.

/s/Patrick J. Hennessey, Jr.
PATRICK J. HENNESSEY, JR.
Attorney for Defendant

PROOF OF SERVICE BY MAIL/ELECTRONIC SERVICE SUBMISSION

I, the undersigned, declare that: I am over the age of eighteen years and not a party to the action; I am employed in the County of San Diego, California, within which county the subject mailing occurred; my business address is 2356 Moore Street, Suite 201, San Diego, California; I am familiar with this firm's practice for collection and processing correspondence for mailing with the United States Postal Service pursuant to which practice all correspondence will be deposited with the United States Postal Service the same day in the ordinary course of business. I served the following document(s):

Appellant's Opening Brief

by placing a copy thereof for each addressee named hereafter, addressed to each such addressee, in a separate envelope, postage prepaid, sealed and deposited at this firm's mailstation on 10/26/15 .

Kevin Bollaert
Booking #15707263
446 Alta Road, Ste. 5300
San Diego, CA 92158

San Diego Superior Court
220 West Broadway
San Diego, CA 92101

PROOF OF SERVICE BY ELECTRONIC SERVICE/SUBMISSION
CAL.RULES OF COURT, RULES 2.251(i)(I)(A)-(D) and 8.71(f)(1)(A)-(D)

I server declare I electronically served from my service address the same referenced above document on:

Attorney General
ADIEService@doj.ca.gov

Appellate Defenders Inc.
eservice-criminal@adi-sandiego.com

District Attorney
da.appellate@sdcda.org

I declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct.

Executed on 10/26/15.

/s/PATRICK J. HENNESSEY, JR.
PATRICK J. HENNESSEY, JR.