Filed 6/28/16

CERTIFIED FOR PUBLICATION

COURT OF APPEAL, FOURTH APPELLATE DISTRICT

DIVISION ONE

STATE OF CALIFORNIA

THE PEOPLE, Plaintiff and Respondent, v. KEVIN CHRISTOPHER BOLLAERT, Defendant and Appellant.	D067863 (Super. Ct. No. SCD252338)

APPEAL from a judgment of the Superior Court of San Diego County, David M. Gill, Judge. Affirmed.

Patrick J. Hennessey, Jr., under appointment by the Court of Appeal, for Defendant and Appellant.

Kamala D. Harris, Attorney General, Gerald A. Engler and Julie L. Garland, Assistant Attorneys General, Eric A. Swenson, Junichi P. Semitsu, Garrett A. Gorlitsky, Deputy Attorneys General, and Steven Taylor Oetting, Deputy Solicitor General, for Plaintiff and Respondent.

A jury convicted Kevin Christopher Bollaert of extortion (Pen. Code,[1] § 520; counts 3, 16, 18, 21, 27, 29) and the unlawful use of personal identifying information (§ 530.5, subd. (a); counts 2, 4-15, 17, 19, 20, 22-24, 26, 28), stemming from his operation of Web sites, "UGotPosted.com," through which users posted private, intimate photographs of others along with that person's name, location and social media profile links, and "ChangeMyReputation.com," through which victims could pay to have the information removed. As to some of the victims, the jury unanimously found that Bollaert committed the unlawful act of an invasion of privacy by disclosure of private facts. The trial court declared a mistrial as to one of the identity theft charges (count 25) and a conspiracy charge (count 1). It sentenced Bollaert to a split sentence of 18 years: eight years of local confinement followed by 10 years of mandatory supervision.[2]

Bollaert contends his convictions under section 530.5, subdivision (a) must be reversed for insufficient evidence because (1) he is immunized from liability under section 530.5, subdivision (f) as an "interactive computer service" or "access software provider" within the meaning of the Communications Decency Act (the CDA; 47 U.S.C.

---

1 Statutory references are to the Penal Code unless otherwise specified.

2 The court had initially sentenced Bollaert to 18 years in county jail, consisting of the three-year midterm on count 3, consecutive eight-month terms (one-third the midterm) on counts 4-15, 17, 19, 20, 22-26 and 28, and consecutive one-year terms (one-third the midterm) on counts 16, 18, 21, 27 and 29. The court imposed but stayed under section 654 a two-year midterm on count 2. It later recalled Bollaert's sentence and in September 2015 imposed the split sentence set forth above.

§ 230(c)(1));[3] (2) he did not take action to develop or create the content of his Web site, and therefore was not liable as an "information content provider" as defined by the CDA; and (3) he did not willfully obtain the personal identifying information for an unlawful purpose. Bollaert further contends there is insufficient evidence supporting his extortion convictions because he did not directly or implicitly threaten any of the victims to expose any secret; the alleged secrets—the photographs—were already in the public domain; and he merely engaged in a business practice whereby legally posted information could be removed. Finally, Bollaert contends the trial court erred by giving the jury instructions on civil liability—CACI Nos. 1800 and 1801—regarding intrusion into private affairs and public disclosure of private facts.

We conclude the evidence is sufficient to support Bollaert's convictions for unlawful use of personal identifying information as well as extortion, and that the jury's rejection of CDA immunity is likewise supported by evidence that Bollaert developed, at least in part, the offensive content on his Web site by requiring users to input private and personal information as a condition of posting the victims' pictures, making him an information content provider within the meaning of the CDA. We further conclude Bollaert invited the claimed instructional error, but hold in any event that he has not shown error in the instructions as a whole. We affirm the judgment.

---

[3] References to title 47 United States Code section 230 will at times be referred to as section 230.

FACTUAL AND PROCEDURAL BACKGROUND[4]

In 2012, 2013 and 2014, a number of individuals discovered that photographs of themselves, including nude photographs, as well as their names, hometowns, and social media addresses, had been posted without their permission on a Web site, UGotPosted.com. Most of the pictures were taken by or for former significant others or friends.[5] Some of the pictures the victims had taken on their own phones or placed on personal webpages for private viewing by themselves or select others. Some had been taken while the victim was drugged and in a compromised state or otherwise unaware of the photographing. Victims received harassing and vulgar messages from strangers. Many of the victims contacted the Web site administrator at UGotPosted.com to try to get their photographs and information removed without success. One of the victims testified that when she tried to communicate with the UGotPosted contact, she reached a person named "James Smith," not realizing it was Bollaert, who told her that to remove her photos she would have to provide two forms of identification and show an unspecified sign. The UGotPosted Web site contained a link to another Web site, ChangeMyReputation.com, where victims were told that for payment of a specified amount of money, their pictures and information would be taken down. Six of the

---

[4] Some of the factual background is taken from a surreptitiously taped interview of Bollaert by special agents with the Department of Justice, which was played to the jury at trial.

[5] One witness testified she unwillingly sent the pictures via text to a boy who harassed, stalked and threatened her for the photographs. Two other victims had sent the photographs to another person in connection with a dating application.

victims paid money to an account on ChangeMyReputation.com to have their pictures removed from the Web site.

Bollaert was the administrator and registered owner of the UGotPosted Web site. He created it with another person, Eric Chanson, who eventually declined to participate and transferred his interest to Bollaert. Bollaert was in control of the Web site, and he managed and maintained it; changed, added and deleted content; and updated software that operated the site. He designed the Web site so that he had to review the content before it was posted, and it had "required fields" by which a user who wanted to post pictures of another person had to input that other person's full name, age, location ("city, state, country") and Facebook link. Bollaert had the only user account on the computer; he looked at every single post that came through the Web site and decided what would get posted on it, placed watermarks on each photograph to discourage others from stealing the pictures, and accessed the site remotely. He kept a spreadsheet recording every single post. Bollaert would not post pictures that he deemed "garbage," including pictures that did not include nude persons. He removed pictures of minors and some other content depending on the nature of the request. He moderated and approved the comments that were posted on the Web site, and edited the contents of the posts. At some point, Bollaert received about $800 or $900 in monthly income from advertising off the site. Bollaert felt the Web site was "kinda fun and entertaining" at the beginning, but he later took it down because it was causing him stress and "ruining his life."

Bollaert also set up and managed the Web site ChangeMyReputation.com, to which individuals who had pictures posted on the UGotPosted site would be directed and

told they could pay money to have the information removed. A Department of Justice forensic auditor determined that victims paid a total of $30,147.73, which eventually was forwarded to Bollaert's personal PayPal account. Law enforcement later used Bollaert's site to contact victims. At one point, a legal analyst with the Attorney General's office created a user account and attempted to post pictures of her pet cats on the Web site, but they never appeared.

At trial, the People proceeded on the charges of unlawful use of personal identifying information (§ 530.5, subd. (a)) under three theories: That Bollaert, without authorization, willfully obtained the victims' personal identifying information via the design, maintenance and operation of the Web site UGotPosted.com for the unlawful purpose of annoying or harassing via electronic communication device under section 653m, subdivision (a).[6] Or, that Bollaert, without authorization, willfully obtained the victims' personal identifying information for the unlawful purpose of an invasion of privacy either via public disclosure of private facts, or intrusion into private affairs. Bollaert defended in part on grounds his Web site was an interactive computer service or access software provider expressly immunized under subdivision (f) of section 530.5

---

6 Section 653m, subdivision (a), provides: "Every person who, with intent to annoy, telephones or makes contact by means of an electronic communication device with another and addresses to or about the other person any obscene language or addresses to the other person any threat to inflict injury to the person or property of the person addressed or any member of his or her family, is guilty of a misdemeanor. Nothing in this subdivision shall apply to telephone calls or electronic contacts made in good faith." " 'The purpose of section 653m is to deter people from making harassing telephone calls with the intent to annoy and thus, to secure an individual's right to privacy against unwanted intrusion.' " (*People v. Powers* (2011) 193 Cal.App.4th 158, 164.)

because there was no evidence of intent to defraud, and was also protected under the CDA. The court instructed the jury on these theories and Bollaert's defense at Bollaert's request.[7]

DISCUSSION

I. *Convictions for Unlawful Use of Personal Identifying Information* (*§ 530.5*)

Bollaert contends the evidence is insufficient to support his convictions under section 530.5 under any of the prosecution's theories. He continues to maintain that his Web site is an interactive computer service or access software provider subject to immunity under the CDA and section 530.5, subdivision (f), and that the People presented no evidence he possessed any personal information with the intent to defraud. He further argues that he cannot be an information content provider under the CDA (§ 230, subd. (f)) because in operating the Web site, he "took no action that amounted to developing or creating the content," similar to the defendants who were held immune from tort liability in *Zeran v. America Online, Inc.* (4th Cir. 1997) 129 F.3d 327 (*Zeran*),

---

[7] In addition to CALCRIM No. 2040 as to unauthorized use of personal identifying information, the court instructed the jury with special instruction No. 1 at Bollaert's request. That special instruction reads in part as follows: "The defendant has been prosecuted for the unauthorized use of personal identifying information under three separate theories: (i) violation of Penal Code section 653m; (ii) public disclosure of private facts; and (iii) intrusion into private affairs. Each theory has different requirements as set forth in these instructions. [¶] You may not find the defendant guilty of unauthorized use of personal identifying information unless all of you agree that the People have proved that the defendant committed that crime under at least one of these theories. You do not all need to agree on the same theory." The court also specified the three unlawful purposes required for the unauthorized use of personal identifying information via special instruction No. 2 (violation of section 653m), CACI No. 1800 (intrusion into private affairs) and CACI No. 1801 (public disclosure of private facts).

Carafano v. Metrosplash.com Inc. (9th Cir. 2003) 339 F.3d 1119 (*Carafano*), and *Jones v. Dirty World Entertainment Recordings LLC* (6th Cir. 2014) 755 F.3d 398 (*Jones*).) He additionally argues that with regard to actions not protected by the CDA, there is no evidence he willfully obtained someone else's personal identifying information without that person's consent and used it for an unlawful purpose.

A. *Standard of Review*

The principles governing sufficiency of the evidence claims are "clear and well settled." (*People v. Abilez* (2007) 41 Cal.4th 472, 504.) " 'The proper test . . . is whether, on the entire record, a rational trier of fact could find the defendant guilty beyond a reasonable doubt. [Citations.] On appeal, we must view the evidence in the light most favorable to the People and must presume in support of the judgment the existence of every fact the trier could reasonably deduce from the evidence.' " (*People v. Perez* (2010) 50 Cal.4th 222, 229; *People v. Rangel* (2016) 62 Cal.4th 1192, 1212-1213 [relevant question is " ' "whether, after viewing 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" ' "].) " ' " 'Circumstantial evidence may be sufficient to connect a defendant with the crime and to prove his guilt beyond a reasonable doubt.' " ' " (*People v. Abilez*, at p. 504.) "If the circumstances reasonably justify the trier of fact's findings, reversal of the judgment is not warranted simply because the circumstances might also reasonably be reconciled with a contrary finding." (*People v. Lindberg* (2008) 45 Cal.4th 1, 27.) We may reverse for lack of substantial evidence only if " ' "upon no

hypothesis whatever is there sufficient substantial evidence to support" ' the jury's verdict." (*People v. Zamudio* (2008) 43 Cal.4th 327, 357.)

B. *Section 530.5 and CDA Immunity*

Section 530.5, subdivision (a), proscribes the unauthorized use of personal identifying information (conduct often referred to as "identity theft"). (*People v. Barba* (2012) 211 Cal.App.4th 214, 226; *People v. Hagedorn* (2005) 127 Cal.App.4th 734, 743-744.) It provides: "Every person who willfully obtains personal identifying information, as defined in subdivision (b) of Section 530.55, of another person, and uses that information for any unlawful purpose . . . is guilty of a public offense . . . . " (§ 530.5, subd. (a).) Personal identifying information includes "any name, address [and] . . . date of birth" as well as "unique electronic data including information identification number assigned to the person, address or routing code . . . ." (§ 530.55, subd. (b).) "The elements of the crime defined by the language of the statute may be summarized as follows: (1) that the person willfully obtain personal identifying information belonging to someone else; (2) that the person use that information for any unlawful purpose; and (3) that the person who uses the personal identifying information do so without the consent of the person whose personal identifying information is being used." (*People v. Barba*, at p. 223; see also *People v. Tillotson* (2007) 157 Cal.App.4th 517, 533.)

Subdivision (f) of section 530.5 provides: "An interactive computer service or access software provider as defined in subsection (f) of [the CDA][8] shall not be liable under this section unless the service or provider acquires, transfers, sells, conveys, or retains possession of personal information with the intent to defraud."

In the CDA, Congress declared that "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." (§ 230, subd. (c)(1).) The CDA further states: "No cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section." (§ 230, subd. (e)(3).) These provisions have been held to confer broad immunity against defamation and other civil liability for those who use the Internet to publish information originating from another source. (See *Barrett v. Rosenthal* (2006) 40 Cal.4th 33, 39; *Doe II v. MySpace Inc.* (2009) 175 Cal.App.4th 561, 568; *Fair Housing Counsel of San Fernando Valley v. Roommates.com, LLC* (9th Cir. 2008) 521 F.3d 1157, 1162 (*Roommates*) (en banc); *Carafano*, *supra*, 339

---

8 Under the CDA, an interactive computer service includes an access software provider, though it defines the two separately. The CDA defines an interactive computer service 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." (§ 230, subd. (f)(2).) It defines an access software provider 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 content; [¶] (B) pick, choose, analyze, or digest content; or [¶] (C) transmit, receive, display, forward, cache, search, subset, organize, reorganize, or translate content." (§ 230, subd. (f)(4).) The People do not dispute that the Web site UGotPosted.com is an interactive computer service.

F.3d at p. 1122; *Batzel v. Smith* (9th Cir. 2003) 333 F.3d 1018, 1026; *Zeran*, *supra*, 129 F.3d at pp. 330-331.)

Section 530.5, subdivision (f) sets forth an exemption for interactive computer services or access software providers within the meaning of the CDA, but the California Legislature limited that exemption to interactive computer services that do not act with the intent to defraud. Thus, if an interactive computer service acquires or retains personal identifying information with the intent to defraud, it will be criminally liable under the statute. Under the CDA, however, an interactive computer service likewise loses its immunity if it also functions as an "information content provider" for the portion of the statement or publication at issue. (*Roommates*, *supra*, 521 F.3d at p. 1162; *Carafano*, *supra*, 339 F.3d at pp. 1123, 1125; *Doe II v. MySpace Inc.*, *supra*, 175 Cal.App.4th at p. 568.) The CDA defines an information content provider 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." (§ 230, subd. (f)(3).)

C. *The Evidence Demonstrates Bollaert Willfully Obtained the Victims' Personal Identifying Information and Used It for an Unlawful Purpose*

Before we reach the question of CDA immunity, we address Bollaert's challenge to the evidence supporting the elements of section 530.5 liability. He first argues the evidence does not support a finding that he willfully obtained any personal identifying information of the alleged victims. He points out it was the third parties—ex-boyfriends or personal enemies—who submitted the personal information and maintains he only

"provided the opportunity for third parties to post the information of their choice." According to Bollaert, imposing liability for his conduct would "criminalize the business practice of merely hosting a website." Bollaert further contends there is no evidence he used the identifying information for an unlawful purpose. As we explain, the contentions are meritless.

1. *Willful Conduct*

" 'The word "willfully," when applied to the intent with which an act is done or omitted, implies simply a purpose or willingness to commit the act, or make the omission referred to.' In other words, '[t]he word "willfully" as generally used in the law is a synonym for "intentionally," ' [citation], and ' ". . . implies no evil intent; ' "it implies that the person knows what he is doing, intends to do what he is doing and is a free agent." ' " ' " (*In re Rolando S.* (2011) 197 Cal.App.4th 936, 941.) In *Rolando S.*, the Court of Appeal upheld a petition finding a minor willfully obtained personal identifying information of another in violation of section 530.5—the victim's e-mail account password—even though the minor had received the password in an unsolicited text message, and then accessed the victim's Facebook page to write "sexually explicit and vulgar comments on the victims' [*sic*] friends' walls, accessible by the victims' [*sic*] friends and acquaintances," thereby "clearly expos[ing] the victim to hatred, contempt, ridicule and obloquy . . . ." (*Id.* at p. 947.) The court held the minor willfully obtained the password when he chose to remember it and affirmatively used it to gain access to the victim's electronic accounts: "Appellant freely accepted the password information provided in the text message" and "no evidence suggests [he] was forced to remember the

password or otherwise keep a record of it so that he could use it later, as he admitted to doing. . . . [A]ppellant willfully obtained the password information from the text message, knowing that he was continuing to possess the password, intending to do so, and was a free agent when securing the password for his future use." (*Id*. at pp. 941.)

Here, the evidence shows Bollaert designed the UGotPosted Web site for the specific purpose of eliciting nude photographs and private information of other persons; the information was not provided to him by the victims depicted in the photographs whose names and locations were used. Because Bollaert "freely accepted" all of the victims' personal information, intended to continue to possess it, and used it for his own purposes, i.e., for display on his Web site and receipt of advertising income as well as payments from ChangeMyReputation.com, Bollaert willfully obtained the information for purposes of section 530.5. (*In re Rolando S., supra,* 197 Cal.App.4th at p. 941.)

2. *Unlawful Purpose*

We further conclude substantial evidence demonstrates Bollaert obtained and retained the information for an unlawful purpose, namely, to invade the victims' privacy. In *In re Rolando S.*, the court was faced with the minor's claim that he did not use the victim's information for an unlawful purpose, because at most he " 'possibly defamed' the victim" and such civil torts did not meet that standard. (*In re Rolando S., supra,* 197 Cal.App.4th at p. 942.) In addressing that contention, the court examined the legislative history of section 530.5, specifically the 1998 amendment to the statute that added the phrase "any unlawful purpose" (Stats. 1998, ch. 488, § 1, p. 3531) and observed that the Legislature "clearly intended to greatly expand the scope of unlawful conduct underlying

the identity theft offense." (*Rolando S.*, at pp. 944-945.) The court applied the California Supreme Court's definition of "unlawful," stating: "Our Supreme Court has defined the term 'unlawful' to include wrongful conduct which is not criminal. In determining the scope of the term, it held that an act is 'unlawful . . . if it is proscribed by some constitutional, statutory, regulatory, common law, or other determinable legal standard. [Citations.]' [Citation.] Under this definition, unlawful conduct includes acts prohibited by the common law or nonpenal statutes, such as intentional civil torts." (*Rolando S.*, at p. 946, citing *Korea Supply Co. v. Lockheed Martin Corp.* (2003) 29 Cal.4th 1134, 1159 & fn. 11; see also *Edwards v. Arthur Andersen, LLP* (2008) 44 Cal.4th 937, 944.)

Thus, the term "unlawful" as used in section 530.5 includes intentional civil torts, including those relied upon by the People here: invasion of privacy by means of intrusion into private affairs and public disclosure of private facts. (See *Shulman v. Group W Productions, Inc.* (1998) 18 Cal.4th 200, 214, 231 (*Shulman*) [discussing elements of both causes of action].) Bollaert does not, in his opening brief, separately address the torts, but rather sets out only the elements of the intrusion tort as the elements of "invasions of privacy." Because he does not address the public disclosure tort or its elements—(1) public disclosure (2) of a private fact (3) that would be offensive and objectionable to the reasonable person and (4) which is not of legitimate public concern (*Shulman*, at p. 214)—on the public disclosure tort theory of unlawful use alone we may affirm Bollaert's 530.5 convictions.

Nevertheless, we conclude substantial evidence supports the jury's verdicts on a theory of invasion of privacy based on intrusion into private affairs. "A privacy violation

based on the common law tort of intrusion has two elements. First, the defendant must intentionally intrude into a place, conversation, or matter as to which the plaintiff has a reasonable expectation of privacy. Second, the intrusion must occur in a manner highly offensive to a reasonable person." (*Hernandez v. Hillsides, Inc.* (2009) 47 Cal.4th 272, 286; see *Shulman, supra*, 18 Cal.4th at p. 231 [" '[o]ne who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person' "].) "To prove actionable intrusion, the plaintiff must show the defendant penetrated some zone of physical or sensory privacy surrounding, or *obtained unwanted access to data about*, the plaintiff." (*Shulman*, at p. 232, italics added.)

Bollaert suggests that liability for this tort would attach only to the third parties who "of their own free will" posted the offensive content without the victim's permission; that he is not responsible because he "could not tell from the submissions whether the people submitting the photos were submitting photos of themselves or other people without their permission." Interpreting this challenge as directed to the intent element, we reject it. As the People point out, the tort is proven where the defendant *obtains unwanted access to private data* about the plaintiff (*Shulman, supra*, 18 Cal.4th at p. 232), and evidence of Bollaert's willful receipt of the intimate photographs from others without the victims' consent meets that standard. Additionally, the evidence contradicts Bollaert's assertions concerning his lack of knowledge, as the evidence shows he required users to post both their own e-mail address, as well as the full name of the victim and the

victim's Facebook link. The People's forensic computer expert testified that Bollaert viewed the Facebook pages of victims on 2,300 occasions, permitting the jury to conclude that Bollaert indeed sought to verify the identity of the persons in the photographs.

Bollaert further suggests the plaintiffs did not have an objectively reasonable expectation of privacy in their photographs, because "[m]ost, 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." He maintains "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." These arguments ignore evidence that two of the victims did not knowingly permit the pictures to be taken but were photographed unbeknownst to them or while they were in a compromised state. It also ignores evidence that Bollaert required users of his site to *also* post other private information in conjunction with the photos: the victims' *full name* and location together, information that many persons would reasonably expect to remain private and not exposed on a public Internet Web site.

As for the victims' photographs themselves, the People correctly point out that complete confidentiality or privacy is not required. The California Supreme Court has recognized limited privacy interests in private communications to others that the press had intercepted for wider dissemination, and its holdings by extension compel the conclusion in this case that the victims' acts of sharing their intimate photographs with a limited number of persons did not extinguish their expectation of privacy as to the Internet or the outside world in general. (See *Sanders v. American Broadcasting*

Companies (1999) 20 Cal.4th 907, 911 [an intrusion cause of action "is not defeated as a matter of law simply because the events or conversations upon which the defendant allegedly intruded were not completely private from all other eyes and ears"]; *Hernandez v. Hillsides, Inc.*, *supra*, 47 Cal.4th at p. 289.) In *Hernandez*, the court, summarizing and quoting its holding in *Sanders*, stated that "privacy expectations can be reasonable even if they are not absolute. '[P]rivacy, for purposes of the intrusion tort, is not a binary, all-or-nothing characteristic. There are degrees and nuances to societal recognition of our expectations of privacy: the fact that the privacy one expects in a given setting is not complete or absolute does not render the expectation unreasonable as a matter of law.' " (*Hernandez*, at p. 289.) Thus, in *Sanders*, where a reporter secretly videotaped and recorded a plaintiff's interactions with other persons in an area that was closed to the public but where coworkers could be seen and heard nearby, the court held the plaintiff could nevertheless have a cause of action for invasion of privacy by intrusion based on the reporter's covert videotaping. (*Sanders*, 20 Cal.4th at pp. 914, 917-918, 923.) "Defendants' claim, that a 'complete expectation of privacy' is necessary to recover for intrusion, . . . fails as inconsistent with case law as well as with the common understanding of privacy. Privacy, for purposes of the intrusion tort must be evaluated with respect to the identity of the alleged intruder and the nature of the intrusion. . . . [A]n employee may, under some circumstances, have a reasonable expectation of visual or aural privacy against electronic intrusion by a stranger to the workplace, despite the possibility that the conversations and interactions at issue could be witnessed by coworkers or the employer." (*Id.* at pp. 917-918; see also *id.* at p. 923 ["the possibility of

being overheard by coworkers does not, as a matter of law, render unreasonable an employee's expectation that his or her interactions within a nonpublic workplace will not be videotaped in secret by a journalist"].)

In this case, there is no question based on the evidence concerning the inherently personal nature of the images, the testimony of the victims who sent their images only to another person or select others, the victims' generally shocked and horrified reaction to the display of those images on Bollaert's Web site, and their attempts to get them removed, that the jury could conclude each of those victims reasonably expected his or her images to be private as to that person or persons to whom they were sent.

Given the foregoing conclusions, we need not decide whether the evidence is likewise sufficient to support Bollaert's section 530.5 conviction on the theory he acted with the unlawful purpose to annoy or harass the victims by means of an electronic communication device in violation of section 653m, subdivision (a). Even if we were to assume arguendo the People's theory of unlawful purpose under section 653m, subdivision (a) was unsupported by the evidence, we may uphold Bollaert's convictions on the other two theories. This court has stated: "[I]f a jury is presented with multiple theories supporting conviction on a single charge and on review one theory is found unsupported by sufficient evidence, reversal is not required if sufficient evidence supports the alternate theory and there is no affirmative basis for concluding the jury relied on the factually unsupported theory because it is presumed jurors would not rely on a factually deficient theory." (*People v. Llamas* (1997) 51 Cal.App.4th 1729, 1740, citing *People v. Guiton* (1993) 4 Cal.4th 1116, 1128-1129.) The California Supreme Court in

Guiton explained that "[i]f the inadequacy of proof is purely factual, of a kind the jury is fully equipped to detect, reversal is not required whenever a valid ground for the verdict remains, absent an affirmative indication in the record that the verdict actually did rest on the inadequate ground." (*Guiton*, 4 Cal.4th at p. 1129.) Bollaert has not pointed to any such affirmative indication in the record, and we find none.

D. *The Evidence Is Sufficient to Support Bollaert's Convictions Under 530.5 Regardless of CDA Immunity Because There Is Evidence from Which the Jury Could Reasonably Find Bollaert Retained or Acquired Personal Information with the Intent to Defraud*

Bollaert contends the People presented no evidence supporting their claim that he possessed personal information with the intent to defraud by operating the ChangeMyReputation Web site so as to deceive victims into thinking they were paying money to a Web site unconnected with UGotPosted. Bollaert points out that his UGotPosted Web site contained a link to ChangeMyReputation.com, showing he was not hiding the connection between the sites, and that one victim testified it was "obvious" to her that the same person was behind both sites. He maintains the victims paid money because they wanted their pictures removed, not because they were deceived.

"An intent to defraud is an intent to deceive another person for the purpose of gaining a material advantage over that person or to induce that person to part with property or alter that person's position by some false statement or false representation of fact, wrongful concealment or suppression of the truth or by any artifice or act designed to deceive." (*People v. Pugh* (2002) 104 Cal.App.4th 66, 72, citing *People v. Booth* (1996) 48 Cal.App.4th 1247, 1253.) In *Booth*, the court further explained: " ' "Intent to

defraud is an intent to commit a fraud." [Citation.] " 'Fraud' and 'dishonesty' are closely synonymous. Fraud is defined as 'a dishonest stratagem.' [Citation.] It 'may consist in the misrepresentation or the concealment of material facts' [citation], or a statement of fact made with 'conscious[ness] of [its] falsity.' " ' " (*Booth*, at p. 1253.) This court has recently held that to "defraud" means " 'to injure someone in their pecuniary or property rights.' " (*People v. Isom* (2015) 240 Cal.App.4th 1146, 1150, quoting *Lewis v. Superior Court* (1990) 217 Cal.App.3d 379, 393-394.)

Specific intent to defraud is often proven by circumstantial evidence; it is thus typically inferred from all of the facts and circumstances. (*People v. Williams* (2013) 218 Cal.App.4th 1038, 1066, citing *People v. Abilez*, *supra*, 41 Cal.4th at p. 508; *People v. Smith* (1998) 64 Cal.App.4th 1458, 1469; *People v. Wilkins* (1972) 27 Cal.App.3d 763, 773; *People v. Hambleton* (1963) 218 Cal.App.2d 479, 482 ["The intent to defraud can be inferred from all the facts and need not be proved by direct evidence"].) Furthermore, "[p]roof of a false factual representation need not be by words alone; it may be implied from conduct; it may be made either expressly or by implication; the form of the words in which the pretense is couched is immaterial; if the words or conduct are intended to create the impression that defendant is making a representation as to a present fact, the pretense is within the statute." (*People v. Brady* (1969) 275 Cal.App.2d 984, 996; see also *People v. Reed* (1961) 190 Cal.App.2d 344, 353.)

Here, the evidence showed that when many of the victims e-mailed the webmaster contact at UGotPosted.com and pleaded to have their personal information removed, they received no response. For at least one victim, Bollaert used a false name when he acted

as the UGotPosted contact person. But victims who contacted and paid ChangeMyReputation.com were successful in their efforts. One victim, Brian, communicated with the e-mail associated with ChangeMyReputation.com to remove his photos and asked whether he could submit payment after his photographs were removed; he received a response telling him, "[W]e can't remove it until you pay." When he expressed his suspicion that the Web sites involved "most likely the same people," the only response he received was a message telling him, "Once it is removed it will not be reposted or we will remove it again." His information was removed after he made his payment. Another victim testified that after receiving no response to her e-mails to UGotPosted, she sent an e-mail to ChangeMyReputation.com and "within minutes" received a response containing payment instructions. Her photographs were removed minutes after she submitted payment. According to another victim, ChangeMyReputation.com purported to remove content from all Web sites, not just UGotPosted.com. She testified she and her ex-boyfriend made two separate payments to ChangeMyReputation.com; after he made the first payment, her photographs appeared again on other Web sites and she then paid an additional amount to have those photographs removed.

We conclude based on all of these facts, that the circumstantial evidence was sufficient for a jury to find Bollaert acquired and retained all of the victims' personal identifying information with the intent to defraud. That is, Bollaert purposely set up UGotPosted.com so that it directed victims to an entirely separate Web site where they could remove the content for a fee; he named the Web sites differently and used different

e-mail addresses, suggesting he intended to conceal the fact the Web sites were operated by the same person and induce victims to believe they were making the payment to a different entity; he at times used a pseudonym and never disclosed the Web sites were operated by the same person despite at least one victim expressing his suspicion that such was the case; and he thereby duped the victims into paying money to him, the very same operator of the UGotPosted Web site, unbeknownst to them. It was only after payment that he would remove the offensive content. It is of no moment that one victim was not fooled, but believed correctly that the Web sites were operated by the same person, as the evidence must demonstrate only Bollaert's fraudulent intent, not actual success in his efforts. (*People v. Reed*, *supra*, 190 Cal.App.2d at p. 353 [intent to defraud does not require reliance by the person intended to be defrauded as does actual fraud].) The fact there is evidence from which a finder of fact could decide to the contrary does not require a different result on our review for substantial evidence.

Under section 530.5, subdivision (f), Bollaert's status as an interactive computer service or access software provider is irrelevant if Bollaert acted with the intent to defraud. Thus, the jury's finding that Bollaert acted with the intent to defraud renders it unnecessary for us to proceed to the question of CDA immunity, including to decide whether Bollaert's actions make him an information content provider, taking him outside CDA immunity. We in any event address that question under this unique set of facts, the resolution of which requires us to uphold the jury's verdicts on Bollaert's section 530.5 convictions.

E. *The Evidence Is Sufficient to Support the Jury's Finding That Bollaert Is an Information Content Provider Not Immunized by the CDA*

At both parties' request, the court instructed the jury that section 530.5, subdivision (f) would not apply to Bollaert if he were also an information content provider. The jury was additionally instructed at Bollaert's request that "[a]n interactive computer service or access software provider can become an 'information content provider' to the extent a website is designed to require users to post illegal or actionable content as a condition of use." Also at Bollaert's request the jury was told that certain actions—"[c]hoosing which third party submissions to publish or not publish on a website," "[e]diting third party submissions," "[a]dopting or ratifying third party submissions," or "[e]ncouraging defamatory or actionable third party submissions"—would not by themselves make a person an information content provider. Bollaert concedes on appeal that an information content provider does not receive CDA immunity.[9]

In arguing he cannot be an information content provider subject to liability, Bollaert compares his conduct to that of the defendants in *Zeran, supra*, 129 F.3d 327, *Carafano, supra*, 339 F.3d 1119 and *Jones, supra*, 755 F.3d 398, who were held to fall

---

9 Given Bollaert's concession below that an information content provider is not an interactive computer service, rendering it subject to liability for unlawful use of personal identifying information under section 530.5, we have no occasion to address whether the California Legislature intended to incorporate "information content provider" liability within section 530.5 regardless of the existence of evidence of the defendant's intent to defraud.

within the scope of CDA immunity. As we explain, we reject these comparisons, and hold that Bollaert's design and operation of UGotPosted.com—which required users who wished to use the Web site to provide content that violated other persons' privacy—does not entitle him to statutory immunity under the CDA. We base our conclusion on the reasoning of the Ninth Circuit Court of Appeals in *Roommates*, *supra*, 521 F.3d 1157, which Bollaert mentions but does not discuss in any detail in his opening brief.

In *Roommates*, *supra*, 521 F.3d 1157, the defendant Web site, Roommate.com (Roommate), matched potential landlords and renters, while collecting a profit from advertisers and subscribers. (*Id*. at p. 1161.) As the Ninth Circuit en banc majority described it: "Before subscribers can search listings or post housing opportunities on Roommate's website, they must create profiles, a process that requires them to answer a series of questions. In addition to requesting basic information—such as name, location and e-mail address—Roommate requires each subscriber to disclose his sex, sexual orientation and whether he would bring children to a household. Each subscriber must also describe his preferences in roommates with respect to the same three criteria: sex, sexual orientation and whether they will bring children to the household. The site also encourages subscribers to provide 'Additional Comments' describing themselves and their desired roommate in an open-ended essay. After a new subscriber completes the application, Roommate assembles his answers into a 'profile page.' The profile page displays the subscriber's pseudonym, his description and his preferences, as divulged through answers to Roommate's questions." (*Id*. at p. 1161.) The plaintiff sued defendant for violations of the Fair Housing Act (FHA) and California's fair housing laws

prohibiting discrimination on the basis of race, familial status or national origin (see *Doe II v. MySpace, Inc.*, *supra*, 175 Cal.App.4th at p. 574), but the district court dismissed the federal claims on summary judgment, ruling the defendant was immune under section 230(c) of the CDA. (*Roommates*, 521 F.3d at pp. 1161-1162 & fn. 1.)

On appeal, the plaintiff argued that the defendant violated the FHA and analogous California law by posing illegal questions during the registration process, and also by requiring the subscribers to answer the questions as a condition of using defendant's services. (*Roommates*, *supra*, 521 F.3d at pp. 1164, 1165.) The Ninth Circuit agreed that Roommate was an "information content provider" within the meaning of the CDA as to the questions it posed: the defendant "created the questions and choice of answers, and designed its website registration process around them" and thus could not claim CDA immunity for posting the questions on its Web site or for forcing subscribers to answer them as a condition of using its services. (*Id.* at p. 1164.) The court pointed out that a party responsible for putting information online may be subject to liability even if the information originated with a user. (*Id.* at p. 1165, citing *Batzel v. Smith*, *supra*, 333 F.3d at p. 1033.) It explained, "By requiring subscribers to provide the information as a condition of accessing its service, and by providing a limited set of pre-populated answers, Roommate becomes much more than a passive transmitter of information provided by others; it becomes the developer, at least in part, of that information. And section 230 provides immunity only if the interactive computer service does not 'creat[e]

or develop[]' the information 'in whole or in part.' " (*Roommates*, at p. 1166.)[10] It held the defendant was "sufficiently involved with the design and operation of the search and e-mails systems—which are engineered to limit access to housing on the basis of the protected characteristics elicited by the registration process—so as to forfeit any immunity to which it was otherwise entitled under section 230." (*Id*. at p. 1170.)

In reaching its conclusions, the Ninth Circuit majority declined to read the statutory term "development" so narrowly as to apply only to content that originated entirely with the Web site. (*Roommates*, *supra*, 521 F.3d at p. 1167.) "We believe that both the immunity for passive conduits and the exception for co-developers must be given their proper scope and, to that end, we interpret the term 'development' as referring not merely to augmenting the content generally, but to *materially contributing* to its alleged unlawfulness. In other words, a Web site helps to develop unlawful content, and thus falls within the exception to section 230, if it contributes materially to the alleged illegality of the conduct." (*Id*. at pp. 1167-1168, italics added.)

It also clarified its reasoning in *Carafano, supra*, 339 F.3d 1119, which Bollaert sees as analogous. In *Carafano*, the question was whether the defendant dating service Web site was statutorily immune under the CDA for false content in a dating profile

---

10 The Ninth Circuit majority rejected the dissent's view that defendant merely provided a " 'form with options for standardized answers' " and thus did not develop the information: "[Defendant] does much more than provide options. . . . [I]t asks discriminatory questions that . . . are not entitled to CDA immunity. . . . The FHA makes it unlawful to ask certain discriminatory questions for a very good reason: Unlawful questions solicit (a.k.a. 'develop') unlawful answers. Not only does [defendant] ask these questions, [it] makes answering the discriminatory questions a condition of doing business." (*Roommates*, *supra*, 521 F.3d at p. 1166.)

provided by someone posing as the celebrity plaintiff. (*Id*. at p. 1120.) The dating Web site gave users a "detailed questionnaire" that included multiple-choice questions wherein "members select answers . . . from menus providing between four and nineteen options," including some sexually suggestive answers. (*Id.* at p. 1121.)[11] The profile at issue included the plaintiff's home address and telephone number, causing the plaintiff to receive sexually explicit and threatening messages and calls. (*Id*. at pp. 1120-1121.)

The Ninth Circuit in *Carafano* held the defendant could not be considered an information content provider and thus was immune under the CDA. (*Carafano*, *supra*, 339 F.3d at pp. 1124-1125.) The court pointed out that the CDA immunized an electronic newsletter operator even though the operator selected for publishing a defamatory e-mail under the CDA (*id*. at p. 1123, discussing *Batzel v. Smith*, *supra*, 333 F.3d at pp. 1030-1032), and "so long as a third party willingly provides the essential published content, the interactive service provider receives full immunity regardless of the specific editing or selection process." (*Carafano*, at p. 1124.) As to the dating service defendant in *Carafano*, "[t]he fact that some of the content was formulated in response to [defendant's] questionnaire does not alter this conclusion. Doubtless, the questionnaire facilitated the expression of information by individual users. However, the selection of the content was left exclusively to the user. The actual profile 'information' consisted of the particular options chosen and the additional essay answers provided.

---

11 Notably, the service's policies prohibited members from posting last names, addresses, phone numbers, or e-mail addresses within a profile, and also reviewed the photographs, but not the profiles, for impropriety before posting them. (*Carafano*, *supra*, 339 F.3d at p. 1121.)

[Defendant] was not responsible, even in part, for associating certain multiple choice responses with a set of physical characteristics, a group of essay answers and a photograph. [Defendant] cannot be considered an 'information content provider' under the statute because no profile has any content until a user actively creates it." (*Ibid*.)

Pointing to the breadth of the latter statement in *Carafano*, *supra*, 339 F.3d 1119, the majority in *Roommates* disavowed any suggestion that *Carafano* had held an information content provider *automatically* immune so long as the content originated with another information content provider. (*Roommates*, *supra*, 521 F.3d at p. 1171, fn. 31.) It explained, "[E]ven if the data are supplied by third parties, a website operator may still contribute to the content's illegality and thus be liable as a developer. Providing immunity every time a website uses data initially obtained from third parties would eviscerate the exception to section 230 for 'develop[ing]' unlawful content 'in whole or in part.' " (*Id*. at p. 1171.) The Ninth Circuit clarified that in *Carafano*, the defendant was immune because "[t]he allegedly libelous content there—the false implication that [the plaintiff] was unchaste—was created and developed entirely by the malevolent user, without prompting or help from the website operator." (*Roommates*, at p. 1171.) Though the defendant provided "neutral tools" used by the poster, it "did absolutely nothing to encourage the posting of defamatory content—indeed, the defamatory posting was contrary to the website's express policies. . . . With respect to the defamatory content, the website operator was merely a passive conduit and thus could not be held liable for failing to detect and remove it." (*Id*. at pp. 1171-1172.)

Carafano's conclusion, the Ninth Circuit held, could not apply to the defendant in *Roommates*: "By contrast, Roommate both elicits the allegedly illegal content and makes aggressive use of it in conducting its business. Roommate does not merely provide a framework that could be utilized for proper or improper purposes; rather, Roommate's work in developing the discriminatory questions, discriminatory answers and discriminatory search mechanism is directly related to the alleged illegality of the site. Unlike *Carafano* . . . Roommate is directly involved with developing and enforcing a system that subjects subscribers to allegedly discriminatory housing practices." (*Roommates*, *supra*, 521 F.3d at p. 1172.) Furthermore, the Web site in *Roommates* was unlike that in *Carafano* because it was "designed to force subscribers to divulge protected characteristics and discriminatory preferences, and to match those who have rooms with those who are looking for rooms based on criteria that appear to be prohibited by the FHA." (*Ibid*.)

The Ninth Circuit in *Roommates* likewise distinguished *Zeran*, *supra*, 129 F.3d 327, on which Bollaert relies. *Zeran* involved the plaintiff's negligence action against America Online ("AOL") alleging that AOL had "unreasonably delayed in removing defamatory messages posted by an unidentified third party, refused to post retractions of those messages, and failed to screen for similar posting thereafter." (*Zeran*, *supra*, 129 F.3d at p. 328.) The Ninth Circuit in *Roommates* observed that the Fourth Circuit in *Zeran* held AOL immune under the CDA for the defamatory and harassing message board postings, pointing out that "AOL did not solicit the harassing content, did not encourage others to post it, and had nothing to do with its creation other than through

AOL's role as the provider of a generic message board for general discussions." (*Roommates*, *supra*, 521 F.3d at p. 1172, fn. 33.) We agree there is no indication that AOL in that case acted as anything other than a passive conduit for the allegedly harmful content.

Here, the evidence shows that like the Web site in *Roommates*, Bollaert created UGotPosted.com so that it forced users to answer a series of questions with the damaging content in order to create an account and post photographs. That content—full names, locations, and Facebook links, as well as the nude photographs themselves—exposed the victims' personal identifying information and violated their privacy rights. As in *Roommates*, but unlike *Carafano* or *Zeran*, Bollaert's Web site was "*designed to solicit*" (*Roommates*, *supra*, 521 F.3d at p. 1170, italics added) content that was unlawful, demonstrating that Bollaert's actions were not neutral, but rather materially contributed to the illegality of the content and the privacy invasions suffered by the victims. In that way, he developed in part the content, taking him outside the scope of CDA immunity.

Bollaert would have us follow the Sixth Circuit's decision in *Jones*, *supra*, 755 F.3d 398, involving a "user-generated, online tabloid" where users could anonymously post comments, photographs and video, which the operator selected and published along with his own editorial comments. (*Id*. at pp. 401-402.) But *Jones* supports our conclusions. There, the Sixth Circuit adopted the Ninth Circuit's material contribution test to determine whether a Web site operator is " 'responsible, in whole or in part, for the creation or development of [allegedly tortious] information' " within the meaning of the CDA. (*Id*. at p. 413.) The court held that unlike the Web site in *Roommates*, the Web

site operator in that case "did not require users to post illegal or actionable content as a condition of use," but instead instructed users to " '[t]ell us what's happening' " and " 'who, what, when, where, why.' " (*Id*. at p. 416.) It also provided "*neutral* tools"—labels by which to categorize the submission—as to what third parties submit. (*Id*. at p. 411.) These tools, the Sixth Circuit held, did not constitute a material contribution to any defamatory speech that was uploaded. (*Ibid*.) Nothing in *Jones* changes our conclusion that the evidence in this case supports the jury's finding that Bollaert's design and operation of UGotPosted.com made him an information content provider, taking him outside CDA immunity.

II. *Sufficiency of Evidence of Extortion*

Bollaert contends the evidence is insufficient to support his convictions for extortion. He reiterates the People's extortion theory: that he threatened to injure the victims by publishing their images on his UGotPosted Web site and used the postings to illegally obtain money via ChangeMyReputation.com by having the photos removed. Bollaert does not challenge evidence of his specific intent to extort; rather, he maintains that as an interactive computer service provider and access software provider, he was under no legal obligation to remove third party postings from his Web site even if they were negative, but instead "merely offered a service to remove the photos." According to Bollaert, he was "engaging in standard business practice," and not extortion, similar to the practices approved by the Ninth Circuit in *Levitt v. Yelp!, Inc.* (9th Cir. 2014) 765 F.3d 1123 (*Levitt*). Bollaert also contends there is no evidence he directly or impliedly threatened any of the victims, and that the information, which was already publicly

available and exposed on his Web site, cannot constitute a secret for purposes of extortion.

The People respond that Bollaert used the implicit threat of *continued* exposure of the victims' pictures and information to extort money from them, and because his Web site contained, and indeed required, posters to provide the victims' personal identifying information, he was obligated to remove the content. Relying on *People v. Peniston* (1966) 242 Cal.App.2d 719, the People further respond that a secret can remain a secret despite being made known to others, even many others, as long as there are some who do not know it. They distinguish the circumstances here from those in *Levitt, supra*, 765 F.3d 1123 and assert the Ninth Circuit's analysis in that case is not controlling or persuasive on the question of whether Bollaert should be immune from liability under the CDA.

A. *Trial Evidence*

At trial, victim Rebecca testified that after her manager at work had been told one of his employees "was doing suspicious activity on the Internet," she discovered that intimate photographs of herself and her ex-fiancée, as well as her full name, work location, Facebook link and age, were posted on UGotPosted.com without her consent. Rebecca felt "extremely violated" by the situation, which was very hurtful and embarrassing to her. She e-mailed the Web site and demanded the photographs be taken down, but received no response. She also e-mailed ChangeMyReputation.com, and within minutes received a response directing her to pay $249.99 via PayPal. Rebecca paid the money because she felt the images were disgusting and, though her manager and

others had already seen them, she was worried the images would be exposed to more people.

Victim Jennifer testified that after she discovered nude pictures of her had been posted to UGotPosted.com without her consent (in addition to her full name and work location) she e-mailed the Web site and demanded the content be removed. Based on the e-mails she had sent, as well as the link on UGotPosted.com, she became aware of ChangeMyReputation.com, which Jennifer described as a PayPal account where one could pay money to have the content removed within 48 hours. Jennifer then paid $249.99, and her photographs were removed. Jennifer was subjected to racial slurs directed at her as a result of the posting, and she felt "horrible," "dirty," and afraid that someone was going to find her. She was afraid to leave her apartment and missed two weeks of school.

Victim Alaina testified that after she discovered her own nude pictures, full name, age, city and school were posted on UGotPosted.com without her consent, she sent five to 10 messages to the Web site in an effort to have the content removed without response. Alaina testified she then "paid the blackmail fee of $350" to ChangeMyReputation.com, which stated it would take photographs down upon payment. The content was removed the next day. Alaina was "devastated" by the situation; she changed her appearance because she lived in a small town, was afraid of being stalked, and still suffered psychological trauma at the time of trial.

Victim Jasmine testified that she was surprised to find nude pictures of her, her first and last name, and "all of [her] social media" had been placed on UGotPosted.com.

She worked for a large retailer at the time; her employer called to tell her that the company had been informed about her pictures and she would be fired if they were not taken down. Jasmine felt "really embarrassed and ashamed" when she saw the photos, and it was a frightening experience for her because she "didn't want anybody to know." Jasmine paid $249.99 to ChangeMyReputation.com and the content was removed from UGotPosted.com, but her ex-boyfriend had to pay another $249.99 to ChangeMyReputation.com to have the photographs removed from other Web sites where the information later appeared. Nobody from UGotPosted.com ever contacted her about the photographs.

Victim Manuel testified that he was shocked to discover that nude photographs of himself that he had sent to one individual, as well as his full name, town, and Facebook link, had been placed on UGotPosted.com. The situation was upsetting because he was gay and had not informed family or friends to whom the photographs were sent. Strangers submitted commentary and were tracking him, causing him fear and concern. Manuel found the link to ChangeMyReputation.com via a victim's forum and also through UGotPosted.com, submitted a required photograph and a picture of his driver's license, and paid $250 to have the content removed.

Victim Brian testified he was astounded, angry and embarrassed to find his nude pictures, full name, hometown, and Facebook link posted on UGotPosted.com without his consent. He was immediately scared for his job and that his parents would find out about the situation, though they never did learn about it. He e-mailed the Web site administrator at UGotPosted.com. He also e-mailed ChangeMyReputation.com, and

received a response stating: "Once you pay, they will be removed immediately. If not, you can request a refund through PayPal." Brian asked whether he could pay after he was notified the photographs were removed, and received an e-mail stating: "No, we can't remove until you pay." After he expressed concern over possibly sending money to the same operator of UGotPosted.com, he received a response telling him, "Make a payment, and we will remove the content, thanks." After Brian paid $250, the content was removed. The situation caused him shame, embarrassment and stress, as he knew his high school classmates saw the posting and he was worried about who else would see it in the future.

B. *Legal Principles*

"Extortion is the obtaining of property from another, with his consent . . . induced by a wrongful use of force or fear . . . ." (§ 518.) Fear, for purposes of extortion "may be induced by a threat of any of the following: [¶] . . . [¶] . . . To accuse the individual threatened . . . of a crime"; or "[t]o expose, or impute to him . . . a deformity, disgrace or crime" or "expose a secret affecting him [or her]." (§ 519; see *Flatley v. Mauro* (2006) 39 Cal.4th 299, 326.)

"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.' " (*Chan v. Lund* (2010) 188 Cal.App.4th 1159, 1171, quoting *People v. Goodman* (1958) 159 Cal.App.2d 54, 61.) "The 'secret' referred to in the statute is a 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; the secret must affect the threatened person in some way so far unfavorable to the reputation or to some other interest of the threatened person, that threatened exposure thereof would be likely to induce him through fear to pay out money or property for the purpose of avoiding the exposure.' [Citation.] Whether a threatened exposure would have this effect on the victim is a factual question and depends on the nature of the threat and the susceptibility of the victim." (*Philippine Export & Foreign Loan Guarantee Corp. v. Chuidian* (1990) 218 Cal.App.3d 1058, 1978; see also *Cross v. Cooper* (2011) 197 Cal.App.4th 357, 387.)

The threat may be implied from all of the circumstances: " 'No precise or particular form of words is necessary in order to constitute a threat under the circumstances. Threats can be made by innuendo and the circumstances under which the threat is uttered and the relations between [the defendant] and the [target of the threats] may be taken into consideration in making a determination of the question involved.' [Citations.] . . . 'The more vague and general the terms of the accusation the better it would subserve the purpose of the accuser in magnifying the fears of his victim, and the better also it would serve to protect him in the event of the failure to accomplish his extortion and of a prosecution for his attempted crime.' " (*Stenehjem v. Sareen* (2014) 226 Cal.App.4th 1405, 1424; see also *People v. Choynski* (1892) 95 Cal. 640, 642 [persons guilty of extortion "seldom possess the hardihood to speak out boldly and plainly, but deal in mysterious and ambiguous phrases"].)

Extortion is a specific intent crime, and thus guilt depends on the intent of the person who makes the threat and not the effect the threat has on the victim. (*People v. Umana*, *supra*, 138 Cal.App.4th at p. 641.)

C. *The Evidence Is Sufficient to Establish Both a Threat and a Secret Within the Meaning of the Extortion Statute*

We first reject Bollaert's contentions concerning the absence of evidence of any threat or secret for purposes of extortion. Whether the evidence shows Bollaert engaged in the requisite threat by referring victims who desired to remove the offensive content to ChangeMyReputation.com for the purpose of having them pay to remove it, must be analyzed in the entire factual context. (*Stenehjem v. Sareen*, *supra*, 226 Cal.App.4th at p. 1424; *People v. Massengale* (1968) 261 Cal.App.2d 758, 765.) We conclude the threats were inherent and implied in the very structure and content of Bollaert's Web sites, which Bollaert himself created and operated. When victims were directed via UGotPosted.com to the ChangeMyReputation.com Web site, they were informed either via the Web site or e-mail they could have their photos removed for a fee, from which victims could infer that if they did not pay, the offensive content would remain on the site in further public view. Those victims who communicated with Bollaert before they paid were told the content would only be removed upon payment, and Bollaert only removed the content when the victims paid the requested fee, which eventually was deposited in Bollaert's personal account. There is no question based on the victims' testimony that the display of their private images and information subjected them to shame, disgrace and embarrassment as to their reputation and character, and would continue to be exposed to

other people if the content was not removed. The fact Bollaert did not take affirmative action to seek out or contact the victims, but merely responded to the victims' pleas to remove their content, does not render the threat element unsupported by the evidence. Further, as we explain more fully below, Bollaert's act in removing the victims' personal identifying information from his Web site, which he expressly solicited in the first place, did not give him a lawful right to collect a fee.

In sum, there is ample evidence from which the jury could conclude Bollaert's joint operation and connection of the two Web sites in this manner, as well as his communications to the victims, was a means to obtain their money by wrongful use of fear, namely the threat to "impute to [them] . . . disgrace" (§ 519) by continued display of their private nude images and further humiliation, embarrassment, and damage to their reputation, unless they paid.

We further conclude alternatively there is substantial evidence that the victims' photographs and personal identifying information constituted a secret within the meaning of the crime of extortion, notwithstanding its posting on the Internet and viewing by some individuals. We are guided by *People v. Peniston*, *supra*, 242 Cal.App.2d 719. In *Peniston*, the victim, during her relationship with the defendant, gave the defendant partially nude photographs of herself. (*Id*. at p. 721.) After the relationship ended and she married her husband, the defendant returned and asked her to give him money or he would take the pictures to her husband and parents. (*Ibid*.) She paid him, but the defendant contacted her again and when she asked him to return her pictures, he asked for more money, prompting her to go to police. (*Ibid*.) On appeal from his extortion and

attempted extortion convictions, the defendant challenged the evidence supporting the finding that he had threatened to expose a secret, pointing to evidence that the pictures were only some of a number of modeling pictures taken of the victim that had been circulated throughout the West Coast. (*Id*. at p. 722.) The victim had testified her husband knew some pictures existed but not their nature, and neither he nor her mother were aware of her modeling activities. (*Ibid*.) She testified that she was on probation from a prostitution charge and her parents had threatened to remove her children from her if she got into more trouble. (*Ibid*.) She did not want her husband or parents to see the photographs and other motion pictures, which unbeknownst to her had been exhibited in arcades in San Fernando Valley. (*Ibid*.)

The *Peniston* court pointed out that to suffice for extortion, the " 'thing held in secret must be unknown to the general public, *or to some particular part thereof which might be interested in obtaining knowledge of the secret*' " in addition to affecting the threatened person in some way so far unfavorable to the reputation, or to some other interest of the threatened person, that threatened exposure would be likely to induce the victim through fear to pay money so as to avoid the exposure. (*People v. Peniston*, *supra*, 242 Cal.App.2d at p. 722, italics added, quoting *People v. Lavine* (1931) 115 Cal.App. 289, 295; see also *Cross v. Cooper*, *supra*, 197 Cal.App.4th at p. 387.) It held based on the evidence, a trier of fact could reasonably infer the victim feared that disclosure of the pictures to her husband and parents might lead to adverse probation consequences and the loss of her children, making the evidence sufficient to establish a secret within the meaning of section 519. (*Peniston*, at p. 722.) In response to the

defendant's further claim that the motion pictures were not a secret to the general public, the *Peniston* court stated: "We think the trial judge correctly focused on the true issues in the case, whether [the victim's] husband and parents knew about the pictures and whether the threat of disclosure to them put [her] in fear." (*Id.* at p. 723.)[12]

As in *Peniston*, where dissemination of the victim's images to the general public via arcades or other means did not render the evidence insufficient to establish a secret for purposes of extortion because the victim's family had not seen them, here, the fact the victims' photographs were placed on the Internet and exposed to the public did not mean that some other "particular part [of the public]" (*People v. Peniston*, *supra*, 242 Cal.App.2d at p. 722)—namely, family members, classmates, coworkers, or employers who might be interested—had seen them. The People presented direct testimony from some of the six victims concerning their fear that others would see their images if they did not pay to have them removed, as well as evidence as to all of the victims that they quickly paid for removal, from which the jury could readily infer the victims were fearful of continued exposure. The jury could reasonably conclude the photographs therefore remained a secret to persons who had not viewed the Web site, and reasonably found it

---

12 The appellate court also rejected the defendant's contention that there was no evidence of a threat for purposes of his conviction for attempted extortion. It observed that the People had charged him with extortion for his demand for money in November 1963 and attempted extortion in February 1964, and held the latter threat was implied when the defendant told the victim he would return the pictures for $1000: "Although there was no testimony of a direct threat in February, we think both parties understood the consequence of nonpayment to be disclosure to husband and parents. The threat was reasonably inferable from the circumstances." (*People v. Peniston*, *supra*, 242 Cal.App.2d at pp. 723-724.)

was the victims' fear that others would see the content, causing further humiliation or damage to their reputation, that compelled them to pay Bollaert's fee.

Bollaert relies on *Cross v. Cooper, supra,* 197 Cal.App.4th 357 for the proposition that "information publicly available on Web sites 'to anyone interested in knowing about it' " does not constitute a secret within the meaning of the extortion statute. But *Cross* was decided in the context of an anti-SLAPP (Code Civ. Proc., § 425.16) motion, where conclusive evidence of illegal conduct—conduct that is illegal as a matter of law—precludes anti-SLAPP relief. (*Id*. at p. 384.) The court there merely held that the record in that case did not establish *as a matter of law* that the location of a registered sex offender was a secret for purposes of the crime of extortion, partly based on evidence that the information was publicly available on a Web site; plaintiffs' declarations showed she and her neighbors knew of the information; and the plaintiff—who alleged the defendants had interfered with a residential home sale—had conceded she had a duty to disclose to any potential buyer, renter or potential lessee the existence of the Web site containing information about registered sex offenders living in the area. (*Id*. at pp. 387-388.) *Cross* in fact expressly adopted the principle stated in *Peniston* and *Lavine* that a secret may *either* be unknown to the general public or "to some particular part thereof which might be interested in obtaining knowledge of the secret." (*Id*. at p. 387, quoting *Philippine Export & Foreign Loan Guarantee Corp v. Chuidian, supra,* 218 Cal.App.3d at p. 1078 and citing *Peniston, supra,* 242 Cal.App.2d at p. 430 & *People v. Lavine, supra,* 115 Cal.App. at p. 295.) *Cross* does not assist Bollaert.

D. *Bollaert Was Not Engaged in a Legitimate Service or Business Practice*

We further reject Bollaert's claim that he was engaged in a lawful or legitimate business practice and not extortionate conduct. His claim is based on the factual premise, which we have rejected *ante*, that he acted merely as an interactive computer service and thus was not legally required to remove the offensive content, as well as on the Ninth Circuit's decision in *Levitt*, *supra*, 765 F.3d 1123, which he claims discussed "extortion as it relates to Internet service providers [*sic*]."

In *Levitt*, the plaintiff small businesses sued Yelp! Inc. (Yelp), an online forum for persons to express opinions about businesses, claiming it extorted or attempted to extort advertising payments from them including by manipulating or removing positive user-generated reviews about their business. (*Levitt*, *supra*, 765 F.3d at pp. 1126, 1134.) They brought claims for violation of California's Unfair Competition Law (UCL), civil extortion and attempted civil extortion, on the theory Yelp wrongfully threatened them with economic loss. (*Id*. at p. 1127.) Pointing out both the Hobbs Act (18 U.S.C. § 1951(b)(2)) and California law require the obtaining of property with consent induced by a *wrongful* use of force or fear, the Ninth Circuit held the plaintiffs failed to state a claim. It applied a "claim-of-right" defense under which a defendant cannot commit extortion by threatening economic harm to induce a person to pay for a "legitimate service." (*Id*. at pp. 1130 [threat of economic harm made to obtain property from another is not generally considered wrongful where the alleged extortioner has a legitimate claim to the property obtained through such threats], 1133 ["to state a claim of economic extortion under both federal and California law, a 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"].) The court had previously held, for example, that a mobile home park operator does not commit extortion by telling tenants who refused to sign leases that they would have to pay their own utility bills and be subject to future rent increases. (*Id*. at p. 1132, citing *Rothman v. Vedder Park Management* (9th Cir. 1990) 912 F.2d 315.) "[T]he tenants did not allege that the park owner 'may not raise the rent of those who have not signed the lease or that it may not refuse to pay their utility bills,' " and thus they had no "pre-existing right to be free of such threats." (*Levitt*, *supra*, 765 F.3d at p. 1132.) According to the Ninth Circuit, "[a]ny less stringent standard would transform a wide variety of legally acceptable business dealings into extortion." (*Id*. at p. 1133.) Thus, in *Levitt*, the court held in part that the plaintiffs did not allege facts showing Yelp intended to induce payment through an implicit threat of economic harm or the exploitation of economic fears. (*Ibid*.) Plaintiff "had no pre-existing right to have positive reviews appear on Yelp's website"; she did not allege a "contractual right pursuant to which Yelp must publish positive review, nor does any law require Yelp to publish them." (*Ibid*., fn. omitted.)

Bollaert mischaracterizes *Levitt*, which we do not follow in any event. Contrary to Bollaert's suggestion, *Levitt*'s holding did not turn on Yelp's status as an interactive computer service or CDA immunity, which the Ninth Circuit expressly did not address. (*Levitt*, *supra*, 765 F.3d at p. 1129.) The question was whether Yelp's alleged actions were extortionate and thus unlawful under California's UCL. (*Id*. at p. 1130.) Even

assuming arguendo *Levitt* is consistent with California law,[13] as *Levitt* itself pointed out, California does not recognize a claim-of-right defense where a defendant does not threaten "economic loss" or make a threat that involves " 'the exploitation of [economic] fears . . . .' " (*Levitt*, *supra*, 765 F.3d at p. 1133 & fn. 3 [threat to accuse a person of a crime not subject to a claim-of-right defense].) Here, Bollaert's threat was continued exposure of private personal information resulting in a violation of the victims' privacy rights and emotional distress, not a threat to cause them economic harm. Though some victims expressed fear of losing their jobs, Bollaert's threat was not directed to the victims' workplaces or in any way related to their continued employment. Finally, Bollaert's conduct is nothing like the legitimate albeit "hard bargaining" business tactics discussed in *Levitt*. Bollaert, who did not merely decline to remove harmful content but solicited and developed the unlawful content, did not have a lawful right to collect a fee to remove the victims' personal information. And unlike the plaintiffs in *Levitt* who did not have a preexisting right to have positive reviews appear on Yelp's Web site (*id.* at p. 1133), the plaintiff victims here had a preexisting right—under privacy law—to be free of Bollaert's threatened harm and not have their personal identifying information solicited and placed on UGotPosted.com without their consent.

---

13 The California Supreme Court has pointed out that extortion may criminalize a " 'perfectly legal' " threat. (*Flatley v. Mauro*, *supra*, 39 Cal.4th at p. 326; see also *People v. Beggs* (1918) 178 Cal. 79, 84 [belief that the victim owes a debt is not a defense to the crime of extortion; "[i]t is the means employed [to obtain the property of another] which the law denounces"].)

III. *Instruction with CACI Nos. 1800 and 1801*

Bollaert contends the trial court erred when it instructed the jury with CACI No. 1800 pertaining to the tort of invasion of privacy by intrusion into private affairs, and CACI No. 1801 regarding an invasion of privacy by public disclosure of private facts. He argues that because these instructions are based on civil liability and actions arising from civil law obligations, the court "effectively elevated these alleged possible civil wrongs into an unlawful (criminal) purpose to become crucial elements of . . . section 653m[, subdivision] (a)," thereby permitting the jury to consider a lower standard than the beyond-a-reasonable-doubt standard applicable to a criminal offense. He maintains the error was prejudicial because there is no way to determine whether the jury relied on either theory for its convictions on the identity theft counts.

The People respond that Bollaert invited any error regarding these instructions as his counsel requested they be given for a tactical reason. In reply, Bollaert does not challenge the People's position other than to point out that his counsel requested the CACI instruction in response to the court's expressed intention to give some type of civil jury instruction as to the violation of section 653m.

We agree Bollaert's instructional challenge is barred because he invited any assumed error. "Under the invited error doctrine, a defendant cannot complain that the court erred in giving an instruction that he requested. [Citation.] The invited error doctrine applies when the defense has made a ' " ' "conscious and deliberate tactical choice" ' " ' in asking for the instruction in question." (*People v. Merriman* (2014) 60 Cal.4th 1, 104; see also *People v. Scott* (2015) 61 Cal.4th 363, 400 ["Invited error . . . will

only be found if counsel expresses a deliberate tactical purpose in resisting or acceding to the complained-of instruction"].) The rule is designed to prevent a defendant from gaining reversal on appeal because of an error he or she intentionally caused the trial court to make. (*People v. Coffman* (2004) 34 Cal.4th 1, 49.) It will not apply if counsel acted out of ignorance or mistake. (*Ibid.*) If defense counsel takes affirmative action, a clearly implied tactical purpose will suffice to invoke the doctrine. (*Ibid.*)

The record shows that during the jury instruction conference, Bollaert's counsel objected to the People's proposed use of BAJI Nos. 7.20 and 7.21 respectively on the elements of intrusion into private affairs and public disclosure of private facts, but she had submitted the CACI jury instructions and asked the court to use CACI No. 1800 in lieu of BAJI No. 7.20, and CACI No. 1801 in lieu of BAJI No. 7.21. She did so for an expressly tactical purpose, pointing out that the instructions were similar except that CACI No. 1800 contained one element not present in the BAJI instruction: "[W]ith respect to intrusion into private affairs, it contains an element that I wish to argue as the first prong that is not present in the BAJI, which is that the victim had a reasonable expectation of privacy." The People unsuccessfully objected to the use of CACI No. 1800 as overbroad and not in accord with the principles expressed in *Sanders, supra*, 20 Cal.4th 909. As for CACI No. 1801, Bollaert's counsel explained that for purposes of appellate review, she wanted to be consistent and have the most up-to-date version of the instruction. The People expressed no objection to the use of CACI No. 1801. Because Bollaert made a tactical choice to request the CACI instructions, he cannot now be heard to challenge them.

In any event, our agreement with *In re Rolando S., supra,* 197 Cal.App.4th 936 disposes of the premise of Bollaert's challenge, which is that civil wrongs cannot be equated with a "criminal wrong—an unlawful purpose." *Rolando S.* explained in a reasoned analysis that "unlawful conduct includes acts prohibited by the common law or nonpenal statutes, such as intentional civil torts." (*Rolando S.*, at p. 946.)

Bollaert's instructional challenge similarly fails on grounds he has not demonstrated that the instructions *as a whole* were misleading or improper, or that the instructions, the People, or the court somehow suggested or informed the jury that a lesser standard applied. Our role is to determine the correctness of the jury instructions " 'from the entire charge of the court, not from a consideration of parts of an instruction or from a particular instruction.' " (*People v. Castillo* (1997) 16 Cal.4th 1009, 1016.) Here, the trial court instructed the jury accordingly: that they "should not single out or place added emphasis on a particular instruction" but must "consider the instructions as a whole, a complete statement of what the Court considers to be the applicable law." It instructed the jury as to the presumption of innocence and its requirement that the People prove "the truth of what they have alleged" beyond a reasonable doubt. It instructed the jury that the People were required to prove each of the elements of the crime of unauthorized use of personal identifying information beyond a reasonable doubt including the element that Bollaert "willfully used that information for an unlawful purpose"; that Bollaert was being prosecuted for that crime under the People's three separate theories, that "[e]ach of these is a separate theory, legal theory, as to how [Bollaert] committed the crime"; and "[e]ach of them has its own elements, its own

requirements which must be proved beyond a reasonable doubt." Under the circumstances, the jury could not have understood from the instructions given that they were to apply any lesser standard than proof beyond a reasonable doubt to the element of use of personal identifying information for an unlawful purpose, and the various elements of both invasion of privacy theories. Bollaert has not demonstrated instructional error.

DISPOSITION

The judgment is affirmed.

O'ROURKE, J.

WE CONCUR:

McCONNELL, P. J.

HUFFMAN, J.