No. 17-17486

United States Court of Appeals
for the
Ninth Circuit

In re: FACEBOOK, INC. INTERNET TRACKING LITIGATION,

PERRIN AIKENS DAVIS; BRIAN K. LENTZ; CYNTHIA D. QUINN; MATTHEW J. VICKERY,

Plaintiffs-Appellants,

– v. –

FACEBOOK, INC.,

Defendant-Appellee.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA
DISTRICT COURT CASE NO. 5:12-MD-02314-EJD-NC

BRIEF FOR PLAINTIFFS-APPELLANTS [REDACTED VERSION]

LAURENCE D. KING
MATTHEW GEORGE
MARIO M. CHOI
KAPLAN FOX & KILSHEIMER LLP
350 Sansome Street, Suite 400
San Francisco, California 94104
Tel.: (415) 772-4700
Fax: (415) 772-4707

STEPHEN G. GRYGIEL
SILVERMAN THOMPSON SLUTKIN WHITE LLC
201 North Charles Street, 26th Floor
Baltimore, Maryland 21201
Tel.: (443) 909-7516
Fax: (410) 547-2432

FREDERIC S. FOX
DAVID A. STRAITE
RALPH E. LABATON
KAPLAN FOX & KILSHEIMER LLP
850 Third Avenue, 14th Floor
New York, New York 10022
Tel.: (212) 687-1980
Fax: (212) 687-7714

Attorneys for Plaintiffs-Appellants

TABLE OF CONTENTS

Page(s)

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Rules

Other Authorities

Constitutional Provisions

INTRODUCTION

"For every wrong, there is a remedy."

- Cal. Civ. Code § 3523, enacted in 1872.

Six and a half years ago, Defendant-Appellee Facebook, Inc. ("Facebook") was caught secretly tracking its subscribers' valuable and intensely private personally-identifiable web browsing even after the subscribers had logged out of their accounts. More than a year prior, however, Facebook had explicitly represented and promised that only *logged-in* subscribers consented to being tracked. Public outrage immediately followed; privacy advocates demanded action; and Congress investigated. Facebook apologized and altered its data collection practices. The Federal Trade Commission ("FTC") and Facebook entered into a privacy consent decree agreeing to an unprecedented 20 years of privacy audits, and a multi-district litigation was created following the filing of more than two dozen class actions. But even with the benefit of limited confidential discovery conclusively demonstrating that Facebook was aware of the problem for more than a year before fixing it, and suggesting a strong financial motive for the secret practice,[1] the District Court below found as a matter of law that the victims have no remedy.

[1] Text highlighted in YELLOW reflects or quotes from material sealed by the District Court below.

On April 22, 2010, Facebook launched the "Like" button outside of the Facebook domain. Within weeks it became the single most important social plugin ever created, quickly surpassing Facebook's "Share" button. Less than five weeks after the Like button launch, 50,000 websites had installed it; less than ten weeks after launch, web site consultants were calling it "ubiquitous." By June 2012, a quarter of the top 10,000 websites formally integrated Facebook plugins on their homepages. By November 2013, Facebook claimed on its developer blog that its Like and Share buttons drove more referral traffic than all other social networks combined. Today, Facebook says that web pages containing the Like button and its other plugins are viewed more than 30 *billion* times each day, and more than 7 million websites incorporate them. As the *Huffington Post* summed up, the Like button is now "omnipresent."

When a Facebook subscriber logs into his or her Facebook account, a number of "cookies"—including session cookies and tracking cookies—are written to the user's browser. Several of these cookies can be used to identify the subscriber with specificity. When a subscriber visits a webpage with a Facebook social plugin (such as the Facebook Like button) or a tracking pixel, Facebook's computer code commands the user's browser to re-direct the user's communication, via the file path of the referrer URL of the page being requested, along with all available Facebook tracking and session cookies, to Facebook in real-time. The re-directed

communications are acquired by Facebook regardless of whether the subscriber actually clicks on a Like or Share button or even knows of its existence. Thus, thirty billion times per day, Facebook causes computers around the world to report the real-time Internet communications of more than one hundred million Americans (and more than one billion people globally)—including the entire file path of URLs containing sensitive, personal content—to Facebook. And when Facebook's session and tracking cookies link the URLs to specific persons, anonymity disappears. Facebook can and does link the private web browsing of more than one billion people to their actual identities.

Given the enormous privacy implications of Facebook's ubiquitous insight into web traffic, Facebook assured subscribers that it would not receive user-identifying cookies via its plugins on third-party websites if the subscriber interacts with these websites while *logged out* of Facebook. Facebook made this promise from the first day Facebook launched the Like button. From that day, however, Facebook broke this promise; logging out did not remove all user-identifying cookies and in fact new user-identifying cookies were written to the browsers of logged-out subscribers via the plugins. Discovery has revealed that from the very first day, Facebook knew it was breaching its representations and contractual promises, and chose to keep quiet despite internal concerns.

On September 25, 2011, an independent researcher in Australia publicly revealed that logging out of a Facebook account failed to remove user-identifying cookies—in particular the *c_user*, *lu* and *datr* cookies—allowing Facebook to secretly misappropriate personally identifiable web browsing data of millions of people without consent. The following day (September 26, 2011), the story was picked up by the *Wall Street Journal*, and circulated around the world. Congress demanded (and received) testimony from Facebook, and the FTC investigated. Facebook quickly admitted the problem, and at some point prior to October 3, 2011, issued partial fixes.

The Plaintiffs are four Facebook subscribers whose private web-browsing data was misappropriated by Facebook after April 22, 2010 while the Plaintiffs were logged out of their Facebook accounts. They brought federal privacy claims under Title I of the Electronic Communications Privacy Act ("ECPA") (the "Wiretap Act," 18 U.S.C. § 2510 *et seq*.) and Title II of the ECPA (the "Stored Communications Act," 18 U.S.C. § 2701 *et seq*.).[2] Plaintiffs also brought California common law claims[3] for trespass to chattels, invasion of privacy, intrusion upon seclusion, breach

[2] Plaintiffs also originally brought a third federal claim under the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, but the claim was later dropped.

[3] It is undisputed by any party that California law governs any dispute between subscribers and Facebook, per the terms of the relevant terms and conditions, discussed below.

of contract and breach of the implied covenant of good faith and fair dealing.[4] Finally, Plaintiffs brought state statutory claims under Sections 631 and 632 of the California Penal Code (the California Invasion of Privacy Act, or "CIPA"), Section 502 of the California Penal Code (the Comprehensive Computer Data Access and Fraud Act "CDAFA"), and Sections 484 and 496 of the California Penal Code (Statutory Larceny).[5]

Despite Facebook's remedial measures and apology, and its privacy settlement with the FTC, the District Court nevertheless held that the actual victims have no recourse. The Court dismissed all of Plaintiffs' claims as a matter of law, concluding that more than 100 million Americans are powerless to hold Facebook to account after their personally identifiable web histories were misappropriated. Plaintiffs respectfully request this Court reverse the District Court.

JURISDICTIONAL STATEMENT

The District Court had subject matter jurisdiction over all claims pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The District Court also had subject matter jurisdiction over the federal claims pursuant to 28 U.S.C. § 1331, and

[4] Plaintiffs also originally brought a claim for common law conversion but the claim was later dropped.

[5] Plaintiffs also brought California statutory claims under the California Unfair Competition Law (Calif. Business and Prof. Code § 17200 *et seq*.) and the Consumer Legal Remedies Act (Calif. Civil Code § 1750) but those claims were later dropped.

supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367. On November 17, 2017, the District Court dismissed Plaintiffs-Appellants' claims with prejudice and entered judgment on the same day. *See* Excerpts of Record ("ER"), 2 to 10 (order dismissing Third Amended Complaint); ER1 (Judgment). Plaintiffs timely noticed this appeal on December 14, 2017. ER44 (Notice of Appeal). This Court has jurisdiction pursuant to 28 U.S.C. § 1291.

STATEMENT OF ISSUES PRESENTED FOR REVIEW

1. Whether misappropriation of personally-identifiable data can constitute economic harm under Article III of the United States Constitution absent evidence that the victim's ability to monetize the data was diminished following the misappropriation.
2. Whether, under California law, Plaintiffs sufficiently pled a "reasonable expectation of privacy" in their personally-identifiable aggregated web-browsing history sufficient to sustain claims for Invasion of Privacy and Intrusion Upon Seclusion.
3. Whether, under California law, unauthorized tracking of Plaintiffs' personally-identifiable aggregated web-browsing history can be "highly offensive" to a reasonable person sufficient to sustain claims for Intrusion Upon Seclusion.

4. Whether, under California law, unauthorized tracking of Plaintiffs' personally-identifiable aggregated web-browsing history can be "sufficiently serious" to sustain claims for Invasion of Privacy under the California Constitution.

5. Whether Facebook is a "party to the communication" within the meaning of the Title I of the Electronic Communications Privacy Act (the "Wiretap Act"), 18 U.S.C. § 2510 *et seq*. and California Penal Code Sections 631 and 632 (the California Invasion of Privacy Act, or "CIPA"), when Facebook's computer code commands browsers to automatically send copies of Plaintiffs' personally-identifiable Internet communications to Facebook without the knowledge, action or consent of the Plaintiffs.

6. Whether Plaintiffs adequately pled that their communications with third-party websites are in "temporary storage incidental to transmission" within the meaning of Title II of the Electronic Communications Privacy Act, 18 U.S.C. § 2701 *et seq*. (the "Stored Communications Act"), at the time Facebook caused the communications to be transmitted to Facebook.

7. Whether a personal computer can be a "facility" with the meaning of the Stored Communications Act.

8. Whether Plaintiffs adequately pled a breach of contract under California law.

9. Whether Plaintiffs adequately pled a breach of the implied covenant of good faith and fair dealing under California law.

STANDARD OF REVIEW

Plaintiffs-Appellants seek reversal of the Final Judgment entered in favor of Defendant, ER1, and reversal of portions of the order granting dismissal of the First Amended Complaint ("FAC"), ER25, portions of the order granting dismissal of the Second Amended Complaint ("SAC"), ER11 and portions of the order granting dismissal of the Third Amended Complaint ("TAC"), ER2. This Court reviews the Final Judgment and the orders *de novo*. *Whitman v. Mineta*, 541 F.3d 929, 931 (9th Cir. 2008); *Livid Holdings Ltd. v. Salomon Smith Barney*, 416 F.3d 940, 946 (9th Cir. 2005).

The question presented in a motion to dismiss is whether Plaintiffs are entitled to offer evidence to support their claim, not whether Plaintiffs will prevail. *See Scheuer v. Rhodes*, 416 U.S. 232, 236 (1974), *overruled on other grounds by Davis v. Scherer*, 468 U.S. 183 (1984). In answering that question, the Court accepts Plaintiffs' allegations as true and draws all reasonable inferences in Plaintiffs' favor. *Usher v. City of L.A.*, 828 F.2d 556, 561 (9th Cir. 1987). Even if the chance of recovery is remote, the Court allows Plaintiffs to develop their case "unless the complaint fails to 'state a claim to relief that is plausible on its face.'" *Zucco Partners, LLC v. Digimarc Corp*., 552 F.3d 981, 989 (9th Cir. 2009) (quoting *Bell*

Atl. Corp. v. Twombly, 550 U.S. 554, 570 (2007)); *U.S. v. City of Redwood City*, 640 F.2d 963, 966 (9th Cir. 1981).

STATEMENT OF ADDENDUM

The full text of the relevant statutory provisions is set forth in the statutory addendum included at the end of this brief. *See* 9th Cir. R. 28-2.7.

STATEMENT OF THE CASE AND PROCEDURAL HISTORY

I. Factual Background

The SAC and its exhibits, ER524-ER903, ER1193-ER1315, contain the Plaintiffs' current factual allegations, with the exception of a few additional facts to support the claims for breach of contract and breach of the implied covenant of good faith and fair dealing appearing in the TAC and its exhibits, ER50-ER196, ER1076-ER1192.

A. The Facebook Terms of Service

As alleged in the TAC, Facebook's relationship with its subscribers is governed by the "Statement of Rights and Responsibilities" (the "SRR") and the "Privacy Policy" (later called the "Data Use Policy" but this brief refers to both as the "Privacy Policy" for convenience). ER1082-ER1084. Both documents are contracts, and the Privacy Policy also incorporated by reference additional information on the "Help Center" designed to help subscribers understand how their data is collected and used. The SRR and the Privacy Policy are governed by California law. ER1084-ER1085.

B. URLs Contain the "Contents" of an Electronic Communication

To browse the web via the Internet, users employ a web browser, which is a software application allowing consumers to send, receive and view electronic communications on the Internet and to view the content of web pages. ER1201. Every website is hosted by a server through which it sends and receives communications with Internet users and their web browsers to display web pages on users' monitors and screens, depending on the user's chosen computing device. *Id*. Each website server has an IP address. ER1202. For example, the IP address for the website "www.nytimes.com" is "170.149.161.130." An IP address, however, is not the same thing as a URL. The New York Times website has a single or just a handful of IP addresses for all of the articles, essays, and other content hosted on its webserver. *Id*.

Thus, revealing that an Internet user sent a series of communications to 170.149.161.130 only reveals the parties to the communication – the user and the New York Times. In contrast, a full-string detailed URL reveals both the parties to the communication and the contents of a communication – it reveals the IP address, plus the file path including the name of the article or the search terms (thus, for example, https://www.nytimes.com/2018/01/18/well/live/sex-after-cancer.html).

Although a single webpage appears on a user's screen as a complete product, it is more often an assembled collage of independent parts. ER1203. Some portions

often exist on different servers, often operated by third parties, which send the additional information to a window on the first-party website. ER1204. In essence, the window is a small portion of the third-party's website that peeks through the first-party website, usually in the form of an advertisement or social plug-in. *Id*. To display each part of a single webpage as one complete product, the host server leaves the window blank. Upon receiving a request from a web browser, the Facebook computer code on the website contemporaneously re-directs the web-browser data to Facebook through a separate but simultaneous channel, thereby allowing Facebook to acquire the contents of a user's communication without the user's knowledge or any action on his or her part. *Id*.

In the process of rendering the window, the detailed URL from the first domain is acquired by Facebook. These URLs are called "referrer headers" (technically spelled "referer" due to a quirk of history). *Id*. The re-direction of the referrer URL is accomplished through the individual Internet user's web-browser without any further action or knowledge of the user and occurs both contemporaneously with the user's communications with the first-party website and while the information is in storage by the first-party website and the user's computing device and web-browser. The entire process happens in milliseconds. *Id*.

C. Internet Tracking Through the Facebook "Like" Button

Facebook describes its social plug-ins as a "little piece of Facebook" embedded on a first-party website, as described above. ER1206. When an Internet user lands on a webpage with Facebook computer code, the user's browser is commanded by the Facebook computer code to redirect a copy of the user-to-website communications to Facebook, along with several Facebook cookies. ER1207-ER1208. But the process differs for logged-in users compared to logged-out users and non-subscribers. When a Facebook subscriber is logged into Facebook, the users' browser will contain more than ten Facebook cookies, written to the browser at various times, and several are user-identifying. ER1208-ER1209. When the logged-in subscriber then visits a webpage with a Facebook Like button, a copy of the referrer URL is acquired by Facebook along with the cookies above. ER1209. However, Facebook is not a party to the communication recorded in the referrer URL – instead it acquires a copy of the URL in real time from the user as the page is rendering. No matter how sensitive the website, the referral URL is acquired by Facebook along with the cookies that precisely identify the user. ER1210.

In contrast, when a subscriber logs out of his or her Facebook account, Facebook represented publicly during the class period that it only receives "technical information" about user communications with other websites; when users "log out of Facebook, we remove the cookies that identify your particular account." *Id*.

Facebook still would acquire substantial amounts of data when a logged out user visits a webpage with Facebook functionality – including referrer URLs – but Facebook would not know which person were linked to the URL. Users only consented to Facebook obtaining a copy of the referrer header URL because it was anonymous.

D. Facebook Unlawfully Tracked Logged-Out Subscribers

As soon as the Like button was rolled out on April 22, 2010, Facebook found it had a problem - a large number of users were logging out of their accounts prior to surfing the web. ER1211. Facebook product manager Austin Haugen noted in an internal email dated October 28, 2010, "[redacted]" ER1211; ER1258. A few months later, after reviewing detailed cookie data, Mr. Haugen determined that only approximately "[redacted]" ER1211; ER1278.

The genesis for these discussions was pressure coming directly from [redacted]. In an email dated September 21, 2010, Mr. Haugen wrote: "[redacted]" ER1211; ER1283. Facebook came up with an easy but unlawful interim solution: simply break Facebook's promise to stop tracking users post-logout. This was done

both by failing to delete cookies containing user IDs (such as c_user, lu and fr) and by writing new cookies to the browsers of logged out users. ER1211. Facebook's deception was noticed by some investigators who alerted Facebook. The first was Chris Matyszczyk at CNET, who wrote the following in an email to Facebook spokesman Andrew Noyes on June 4, 2010, just 6 weeks after the launch of the Like button outside the Facebook domain:

> Here's the thing. While everyone has (justifiably, it seems to me) wondered about Facebook forcing people's data into the public domain, I have been alerted to perhaps an even bigger privacy question with respect to the activity feed.
>
> It seems to me that when you visit any page that has a like button, your browser send[s] a request back to Facebook. This means your Facebook cookie can connect you, personally, to your web activity. . . .
>
> Essentially, unlike DoubleClick or an ISP, it seems that you have anointed yourselves with the power to link every Facebook member's web activity with their real personas. Which is a first. And, perhaps, rather scary.

ER1211-ER1212; ER684. The next day, June 5, 2010, a task was created called "[redacted]" Facebook engineering director Alex Himel commented, "[redacted]" ER1212; ER1289.

On June 7, 2010, Mr. Himel created a task with the tag "[redacted]" and assigned it to engineer Chuck Rossi. The task noted:

> [redacted]

[redacted]

[redacted]

ER1212; ER1291. In the following month in July 2010, Mr. Himel [redacted]

[redacted]" but noted in an August 19, 2010 email that changes still had not been made:

[redacted]

ER1213; ER1293. After Mr. Himmel's email above, [redacted]. No attempt was made to delete user-identifying cookies post-logout. These include any of the user cookies (for example, a_user, c_user), the fr cookie, and the lu cookie. This distinction was [redacted] on February 7, 2011: "[redacted]" ER1213; ER1295.

Occasionally during the class period, new[redacted]

[redacted]. ER1213. For example, on January 28, 2011 Alex Himmel noted that [redacted]" ER1213; ER1306. An unknown Facebook employee responded, "[redacted]" *Id.* But the post-logout tracking continued through September 2011.

E. Facebook's Surreptitious Tracking Revealed

On September 25, 2011, Australian researcher and blogger Nic Cubrilovic publicly revealed private research confirming that Facebook was secretly tracking the web browsing of it subscribers who had logged out. ER1220. He wrote, "Even if you are logged out, Facebook still knows and can track every page you visit." He explained that "[t]his is not what 'logout' is supposed to mean- Facebook is only altering the state of the cookies instead of removing all of them when a user logs out." *Id.* Mr. Cubrilovic's blog post spread globally and was picked up the next day by the *Wall Street Journal*, in addition to dozens of other news outlets. ERI221.

Two days after the Cubrilovic revelations, on September 28, 2011, U.S. Representatives Edward Markey and Joe Barton, Co-Chairmen of the Congressional Bi-Partisan Privacy Caucus, submitted a joint letter to the Chairman of the Federal Trade Commission urging the FTC to expand on ongoing investigation of Facebook. ER1222. The FTC had already commenced an investigation related to the Like

button roll-out and changes to the Facebook Privacy Policy in 2010, prior to discovery of the secret and pervasive post-logout tracking. *Id*. Digital privacy rights group EPIC, joined by ten other civil liberties and privacy rights groups had also filed a complaint with the FTC on May 5, 2010 seeking to restrain Facebook's "data collection practices" among other relief, also before knowing about the post-logout tracking. *Id*. The FTC sued Facebook under Section 5 of the FTC Act for multiple counts of misrepresenting its privacy policy, alleging that Facebook engaged in deceptive trade practices. *Id*. (*In the Matter of Facebook Inc*., FTC File No. 0923184). On November 29, 2011, Facebook settled the claims (in a settlement broad enough to encompass the tracking issue), whereby Facebook agreed to an unprecedented 20 years of independent privacy audits. *Id*.

II. Procedural History

Following consolidation of more than two dozen cases with MDL No. 2314, Plaintiffs filed the FAC on May 23, 2012. ER920. On April 11, 2014, the Court entered a stipulated protective order, allowing document discovery to proceed. On October 23, 2015, the District Court dismissed the FAC with leave to replead. ER25. Plaintiffs filed the SAC and Exhibits A through HH partially under seal on December 4, 2015. ER 524 – ER903; ER1193 - ER1315. The Court dismissed the SAC on June 30, 2017, with leave to replead only the claims for breach of contract and breach of the implied covenant of good faith and fair dealing. ER11. Plaintiffs

then filed the TAC (limited to the two claims) partially under seal on August 25, 2017, ER50 – ER196; ER1076 – ER1192. The Court dismissed the TAC with prejudice on November 17, 2017. ER2. Plaintiffs filed a timely notice of appeal on December 14, 2017. ER44.

SUMMARY OF THE ARGUMENT

The legal principles involved in this case are straight-forward. Defendant-Appellee Facebook was caught tracking its subscribers' most intimate web-browsing (and linking the tracking to actual user identity) despite public assurances that users could avoid the tracking by logging out. As learned in discovery, [redacted]. ER1211; ER1258; ER1278. By disregarding the privacy promises made to its subscribers, Facebook may have been able to double its data haul from tens of millions of people. Until the FTC and public pressure put an end to it, it was misappropriation and invasion of privacy on a massive scale.

Yet the District Court found that the victims of Facebook's unlawful actions have no recourse. According to the District Court, data was stolen and Facebook profited therefrom, but the owners of the data suffered no economic harm. Facebook invaded millions of people's privacy, but they had no expectation of privacy anyway, and even if they did, spying on web browsing isn't offensive. Facebook secretly

caused communications to be copied and sent to Facebook, but gets a pass under the Wiretap Act under a view of the "party" exception that most courts reject. These rulings and several others are errors of law that respectfully should be reversed.

ARGUMENT

I. Misappropriation of economically valuable personal data is economic harm even absent evidence of the victim's diminished ability to monetize the data.

In the SAC, the Plaintiffs asserted four claims under California law that specifically "require a showing of economic harm or loss." ER15. These claims are Trespass to Chattels, ER1249; Cal. Penal Code § 502 (the CDAFA), ER1249-ER1250; civil fraud, ER1248-ER1249; and statutory larceny, ER1251-ER1252 (together, the "Economic Loss Claims"). While the District Court properly found Article III standing to pursue all other claims, either based on privacy harms (ER6-ER7) or because of the availability to claim nominal damages (ER7), the District Court found no standing to pursue the Economic Loss Claims. This was an error of law.[6]

[6] It is unsettled whether the dismissal of claims for failure to pled economic loss is a "standing" issue under Rule 12(b)(1) or rather a pleading issue under 12(b)(6) when economic loss is an element of the claim. *See, e.g., See Del Vecchio v. Amazon.com, Inc.*, 2012 WL 1997697, at *2, 9 (W.D. Wash. June 1, 2012) (finding standing, and framing issue under Rule 12(b)(6)). No matter how the issue is framed, however, the analysis below is the same.

The District Court conceded in its Order dismissing the FAC that Plaintiffs sufficiently alleged "that the information collected by Facebook's cookies have economic value and, if the study cited in the [FAC] is accurate, that value may be significant when user information is aggregated. The court accepts as true Plaintiffs' ascription of some degree of intrinsic value to their personal information for this motion." ER34*; see also* Order dismissing SAC, ER16 (citing Order dismissing FAC). In other words, *personal data is property, and it has value*. Taking that data without consent is theft.

Nevertheless, the District Court found that Plaintiffs suffered no "economic loss" when this valuable information was stolen because it was only copied and the victims still retain the data: "In other words, Plaintiffs have not shown, for the purposes of Article III standing, that they personally lost the opportunity to sell their information or that the value of their information was somehow diminished after it was collected by Facebook." ER34.

The District Court's order is contrary to the definition of economic injury under California law. California courts have repeatedly held that economic injury is defined as loss to a victim, *or* unjust profit to a thief. The District Court ignored the second part. As alleged in the SAC, Facebook unlawfully and knowingly failed to delete user-identifying tracking cookies from (and even wrote new ones to) the browsers of its subscribers upon logout. The SAC further alleges that the

unauthorized cookies thus allowed Facebook to gather valuable and private user-identifiable web browsing history, aggregate it, and profit therefrom. It is a textbook example of misappropriation for which the Restatement (Third) of Restitution and Unjust Enrichment (2011) (the "Restatement"), and thus California, defines as injury.

Chapter 1 of the Restatement begins: "A person is not permitted to profit by his own wrong." *Id*. § 3. In the comments, the Restatement holds up this principle as "one of the cornerstones of the law of restitution and unjust enrichment." *Id.*, cmt. a. It almost identically mirrors a similar provision of the California Civil Code, enacted in 1872: "No one can take advantage of his own wrong." Cal. Civ. Code § 3517. Whether one considers Facebook's actions as "trespass to chattels" or "larceny" or "fraud," the remedy is restitutionary or non-restitutionary disgorgement. *See* Restatement, §§ 40 (trespass), 42 (misappropriation); *see also id*., ch. 5 introductory note ("Gains realized by misappropriation, or otherwise in violation of another's legally protected rights, must be given up to the person whose rights have been violated.").

Importantly, the amount of the damages (and thus the amount of the disgorgement) is measured not by any loss to the plaintiffs but by the gain to the defendant. The Restatement is particularly clear on this point, especially when the defendant acts wrongfully rather than innocently. Thus, "the unjust enrichment of a

conscious wrongdoer . . . is the net profit attributable to the underlying wrong. The object of restitution in such cases is to eliminate profit from wrongdoing." *Id*. § 51(4); *id*. § 51, cmt. a ("Recovery so measured may potentially exceed any loss to the claimant."); *id*. § 49(4) ("When restitution is intended to strip the defendant of a wrongful gain, the standard of liability is not the value of the benefit conferred but the amount of the profit wrongfully obtained.").

The bedrock principles noted above are important because California courts have adopted these very provisions of the Restatement when defining economic damages, even though California does not have a separate claim for "unjust enrichment." The California Court of Appeals recently summarized:

> There are two types of disgorgement: restitutionary disgorgement, which focuses on the plaintiff's loss, and nonrestitutionary disgorgement, which focuses on the defendant's unjust enrichment. (*Meister v. Mensinger* (2014) 230 Cal.App.4th 381, 398, 178 Cal. Rptr. 3d 604.) Nonrestitutionary disgorgement is based on sound public policy to prevent a person from benefitting from his/her own wrong at the expense of another "'if the circumstances are such that . . . it is unjust for the person to retain it.'" (Ibid.)
>
> In resolving disgorgement issues, California courts apply principles found in the Restatement Third of Restitution and Unjust Enrichment (Restatement). (*American Master Lease LLC v. Idanta Partners, Ltd*. (2014) 225 Cal.App.4th 1451, 1486, fn. 23, 171 Cal. Rptr. 3d 548.) One such principle, described as "'one of the cornerstones of the law of restitution and unjust enrichment,' [is] '[t]he profit for which the wrongdoer is liable . . . is the net increase in the assets of the wrongdoer, to the extent that this increase is attributable to the underlying wrong.'" (*Id*. at p. 1486.) As the Restatement explains, "The principal focus of [disgorgement] is . . . unjust enrichment . . . measured by the defendant's profits, where the object of restitution is to strip the

> defendant of a wrongful gain [citation]. This [*13] profit-based measure of unjust enrichment determines recoveries against conscious wrongdoers and defaulting fiduciaries." (Rest. 3d Restitution and Unjust Enrichment, § 51, com. a, p. 204.)

City of L.A. v. Mithaiwala, No. B268391, 2017 WL 2858832, at *4–5 (Cal. App. 2d Dist. July 5, 2017), review denied (Sept. 13, 2017); s*ee also Telecom Asset Mgmt., LLC v. FiberLight, LLC*, 203 F. Supp. 3d 1013, 1021 (N.D. Cal. 2016) ("California courts have favorably referenced the new Restatement (Third) of Restitution and Unjust Enrichment"); *Stevenson v. Allstate Ins. Co*., 15-cv-4788-YGR, 2016 WL 1056137, at *14 (N.D. Cal. Mar. 17, 2016) (applying Restatement's "principles of reimbursement" even in absence of claim for unjust enrichment under California law). The District Court erred when it limited the definition of economic damages to losses suffered by the Plaintiffs, when damages must also include unjust gains realized by Facebook. *Meister*, 230 Cal. App. 4th at 398 ("Disgorgement as a remedy is broader than restitution or restoration of what the plaintiff lost.").

In reaching its conclusion, the District Court relied in part on *Low v. Linkedin Corp*., 11-cv-1468-LHK, 2011 WL 5509848 (N.D. Cal. Nov. 11, 2011). Plaintiff Kevin Low challenged LinkedIn's practice of sharing with third-party advertisers certain anonymized records of the profiles viewed by subscribers, and claimed that the value of the data shared amounted to economic damage. As in this case, the *Low* court rejected the "loss of value of data" definition of economic damage. *Id*. at *4-5.

But *Low* should no longer be considered good law. Several years after *Low*, the same judge (the Hon. Lucy Koh) reconsidered the issue in light of recent developments, including in the Ninth Circuit – and held that the loss of value of data (sometimes called "PII" or "personally identifiable information") is economic harm. *See In re Anthem, Inc. Data Breach Litig*., 162 F. Supp. 3d 953 (N.D. Cal. 2016) ("*Anthem I*"). The *Anthem* defendants moved to clarify on the precise question at issue here: does loss of value of data require both that the data have value, **and** that the victim's ability to monetize the data is diminished? In a follow-up opinion, Judge Koh explained: "Plaintiffs are not required to plead that there was a market for their PII *and* that they somehow also intended to sell their own PII." *In re Anthem, Inc. Data Breach Litig*., 15-md-2617-LHK, 2016 WL 3029783, at *15 (N.D. Cal. May 27, 2016) ("*Anthem II*").

There were several reasons for the evolution between *Low* and *Anthem*, not least of which was a summary opinion from the Ninth Circuit allowing fraud claims to proceed against Facebook on a "loss of value of PII" theory. *See In re Facebook Privacy Litig*., 572 F. App'x 494 (9th Cir. 2014). At least one other court in this Circuit has commented on the *Anthem* court's view of the "loss of value of personal information" and found it persuasive and "becoming generally accepted." *In re Premera Blue Cross Customer Data Security Breach Litig*., 3:15-md-2633, 2016 WL 4107717, at *16 (D. Or. Aug. 1, 2016). Because *Anthem II*'s acceptance of the

"loss of value of PII" theory of damages is consistent with the Restatement, consistent with recent authority from the California Court of Appeals, and consistent the Ninth Circuit's summary decision in *In re Facebook Privacy Litig*., the District Court below should be reversed.

II. The Plaintiffs sufficiently pled claims for Intrusion upon Seclusion and Invasion of Privacy under California law.

The elements of a claim for intrusion upon seclusion under California law are (1) intentional intrusion into a place, conversation, or matter as to which the plaintiff had a reasonable expectation of privacy and (2) the intrusion was "highly offensive" to a reasonable person. ER20. A claim for invasion of privacy (enshrined in the California Constitution) includes (1) a specific, legally protected privacy interest, (2) a reasonable expectation of privacy, and (3) a "sufficiently serious" intrusion. *Id*. As noted by the Court below, when a plaintiff asserts both claims, courts conduct a combined inquiry that considers "(l) the nature of any intrusion upon reasonable expectations of privacy, and (2) the offensiveness or seriousness of the intrusion, including any justification and other relevant interests." *Id*.

A. There is a reasonable expectation of privacy in personally-identifiable aggregated web browsing history.

The District Court held as a matter of law that "Plaintiffs have not established that they have a reasonable expectation of privacy in the URLs of the pages they visit." This ruling (if adopted) creates a circuit split on an important issue of

California law; rejects the reasoning of the United States Supreme Court, Congress, the FISA Court and the position of Facebook itself in the analogous Fourth Amendment context; rejects the reasoning of every court in Europe ever to have addressed the issue; prematurely resolves questions of fact at the 12(b)(6) stage; considers (and accepts) facts never appearing in any complaint but instead introduced by Facebook or imported from other cases; and improperly disregards the only ruling on this exact issue by a California state court.

1. The District Court improperly disregarded the ruling of the California Superior Court in the related action Ung v. Facebook.

At the beginning of this MDL, a group of Facebook subscribers in California filed a class action in California state court asserting only state law claims on behalf of California citizens only. *See Ung v. Facebook, Inc*., No. 1-12-cv-217244 (Cal. Super. Ct.); ER1231. Other than the limited focus on California, the class action was (and still is) substantively identical to the MDL. Facebook identified the case as related, and noted the substantial overlap. *See* Notice of Related Action, ER966. Facebook then demurred to the state court complaint.

On July 2, 2012, the Superior Court denied in part and granted in part Facebook's demurrer. ER1231; ER896. On the California invasion of privacy claim, the Superior Court found a legally protected interest in subscribers' browsing histories in the aggregate. ER898. Whether or not there is a reasonable expectation of privacy in a single URL, the court found a reasonable expectation of privacy in

the aggregation of the URLs when linked to user identity. ER899. In particular, the Superior Court found *U.S. v. Maynard*, 615 F.3d 544, 562 (D.C. Cir. 2010), to be "persuasive" because "[e]ven tracking a portion of a person's browsing history . . . can paint a comprehensive picture of a person's life." *Id*. The Superior Court then found the invasion of privacy to be sufficiently serious to sustain a claim under California law. ER901. Like the complaint in *Ung v. Facebook*, the SAC also alleged a privacy interest in the Plaintiffs' aggregated web browsing history, even if not in an individual URL, and a serious invasion of privacy. ER1232, ER1242.

The Plaintiffs appended the Superior Court's *Ung* decision to the SAC. Nevertheless, the District Court rejected the holding in *Ung*, without identifying any basis to conclude that the Superior Court misinterpreted California law. The District Court erred. Under the Rules of Decision Act (Section 34 of the Judiciary Act of 1789), 28 U.S.C. § 725, as applied in *Erie R. Co. v. Tompkins*, 304 U.S. 64 (1938), courts sitting in diversity must apply the substantive law of the state where the court is located. The only court in California ever to address whether Facebook subscribers have a reasonable expectation of privacy in their personally-identifiable browsing history is the Santa Clara County Superior Court. Absent a determination that a higher court might reverse, the District Court should have followed the Superior Court's decision. As the United States Supreme Court held:

> Since our decision in 1938 in *Erie* . . . an unbroken line of cases has held that the federal courts must look to state legislation, state decisions,

> state administrative practice, for the state law that is to be applied. . . . we have never suggested that the federal court may ignore a relevant state court decision because it was not entered by the highest state court. Indeed, we have held that the federal court is obligated to follow the decision of a lower state court in the absence of decisions of the State Supreme Court showing that the state law is other than announced by the lower court.

Commissioner v. Estate of Bosch, 387 U.S. 456, 466 (1967) (internal citations omitted). The Court continued:

> It is true that in *King v. Order of Travelers*, 333 U.S. 153, we held that a federal court of appeals did not have to accept the decision of a state court of common pleas on a matter of state law. But that case was unique. . . . We stressed that our decision was not "to be taken as promulgating a general rule that federal courts need never abide by determinations of state law by trial courts."

Id. at 466-67 (internal citations omitted).

2. The District Court's ruling (if accepted by the Ninth Circuit) would create a circuit split on an important question of California law.

In *In re Google Inc. Cookie Placement Consumer Privacy Litig*., 806 F.3d 125, 151 (3d Cir. 2015) ("*Google Cookie Placement*"), the Third Circuit ruled that Internet users have a reasonable expectation of privacy in their web browsing. The Court analyzed opinions from the United States Supreme Court and from the Foreign Intelligence Surveillance Court to analyze the substance and structure of URLs exchanged between servers whenever a person visits a website. The Third Circuit concluded that URLs can contain "contents" which of course implicate enhanced expectations of privacy in the Fourth Amendment context. *Id*. at 135-39. The court

also noted that the California Supreme Court recognizes the legitimate interests in preventing "unwanted access to data by electronic or other covert means" and the California Constitution protects an interest in "conducting personal activities without observation." *Id*. at 151 (citing *Hernandez v. Hillsides, Inc*., 47 Cal. 4th 272, 285, 287 (2009)). Finally, the Third Circuit noted that defendant Google did not obtain its user data in the ordinary course (as Google argued), but rather through "deceit and disregard." *Id*. at 150. For these reasons, the Third Circuit found a reasonable expectation of privacy.

Similarly, a different panel of the Third Circuit repeated the *Google Cookie Placement* analysis and reached the same conclusion in a different case involving closely analogous New Jersey law. *See In re Nickelodeon Consumer Privacy Litig*., 827 F.3d 262, 295 (3d Cir. 2016) (citing *Google Cookie Placement* and emphasizing that a company's terms of service alone can create reasonable expectations of privacy). The facts of the case at bar are close to *Google Cookie Placement* and *Nickelodeon* – and indeed, Facebook's actions are far more serious because Facebook can link the tracked web history to actual user identity; in *Google* and *Viacom*, the data was anonymous to the collector.

The District Court below implicitly disagreed with both cases, finding no "reasonable expectation of privacy in the URLs of the pages they visit" without

citing to either case[7] or explaining the reason for implicitly rejecting their results. ER21. Therefore, an affirmance of the District Court below would create a circuit split.

3. The District Court rejected the reasoning of the United States Supreme Court, Congress, the FISA Court and the position of Facebook itself in the analogous Fourth Amendment context.

a. ***The Supreme Court's view***: Recent Supreme Court Fourth Amendment jurisprudence reflects the growing and reasonable public desire to be free from electronic surveillance. *See, e.g., United States v. Jones*, 132 S. Ct. 945, 955 (2012) (prolonged electronic location monitoring by government, even in public spaces, violates reasonable privacy expectations). The Supreme Court unanimously extended *Jones* in *Riley v. California*, 134 S. Ct. 2473, 2490 (2014), finding a legitimate privacy interest in aggregated electronic data on a smart phone – ***including Internet web browsing history*** – even if any individual item of data may not give rise to a legitimate interest. "An Internet search and browsing history . . . [can] reveal an individual's private interests or concerns." *Id*. In the same way, Internet users have a reasonable expectation of privacy in the pervasive aggregation of web histories, even if they do not in a single URL.

[7] The District Court did cite to a different portion of *Google Cookie Placement* with approval in ruling that loss of privacy is concrete, intangible "harm" within the meaning of Article III of the United States Constitution and *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540 (2016). ER14. This ruling is not an issue on appeal.

b. ***Congress' view***: In the wake of the events of September 11, 2001, Congress passed the PATRIOT ACT, Pub. L. 107-56, which, among other things, gave the federal government enhanced tools to gather intelligence, including through electronic surveillance of Internet communications. But URLs were specifically identified as being worthy of Constitutional protection precisely because they can contain "contents" within the meaning of the Electronic Communications Privacy Act, and thus implicitly there is an increased expectation of privacy. Restrictions on interceptions of URLs were noted by the House Judiciary Committee in Rept. 107-236 dated October 11, 2001:

> This section updates the language of the [ECPA] to clarify that the pen/register authority applies to modern communication technologies. Current statutory references to the target "line," for example, are revised to encompass a "line or other facility." Such a facility includes: a cellular telephone number; a specific cellular telephone identified by its electronic serial number (ESN); an Internet user account or e-mail address; or an Internet Protocol (IP) address, port number, or similar computer network address or range of addresses. In addition, because the statute takes into account a wide variety of such facilities, section 3123(b)(1)(C) allows applicants for pen register or trap and trace orders to submit a description of the communications to be traced using any of these or other identifiers.
>
> Moreover, the section clarifies that orders for the installation of pen register and trap and trace devices may obtain any non-content information—"dialing, routing, addressing, and signaling information"—utilized in the processing or transmitting of wire and electronic communications. Just as today, such an order could not be used to intercept the contents of communications protected by the wiretap statute. The amendments reinforce the statutorily prescribed line between a communication's contents and non-content information,

> a line identical to the constitutional distinction drawn by the U.S. Supreme Court in *Smith v. Maryland*, 442 U.S. 735, 741-43 (1979).
>
> **Thus, for example, an order under the statute could not authorize the collection of** email subject lines, which are clearly content. Further, an order could not be used to collect information other than ``dialing, routing, addressing, and signaling'' information, such as **the portion of a URL (Uniform Resource Locator) specifying Web search terms or the name of a requested file or article**.

ER389 (emphasis added). If the District Court were correct that citizens have no reasonable expectation of privacy in their URLs, why did Congress specifically single out URLs for protection in the PATRIOT Act, no different than email subject lines and other "content"?

c. ***The FISA Court's view***: In the accompanying Request for Judicial Notice dated March 26, 2018 ("RJN") is a partially declassified (and thus partially redacted) memorandum opinion of the Foreign Intelligence Surveillance Court regarding the "government's application to re-initiate in expanded form a pen register/trap and trace (PR/TT) authorization for the National Security Agency." Memorandum Opinion at 1, RJN219. The NSA argued for expanded collection of bulk Internet communications. *Id*. at 9, RJN227. Consistent with the protections of the Wiretap Act and the U.S. Constitution, the FISA Court restricted the bulk collection of URLs because they can contain "contents," *id*. at 32, RNJ250, meaning there is a higher expectation of privacy than in merely "dialing, routing, addressing and signaling" (DRAS) information. The government argued that a URL should be

considered merely an "address" that "can lead you to a file on any computer on the Internet." *Id*. The FISA Court agreed, but only to the extent the URL were merely an IP address; the court noted that "in some circumstances a URL can also include "contents." *Id*. Citing the PATRIOT Act legislative history above, the Court held that contents can also include that "portion of the URL specifying Web search terms or the name of a requested file or article." *Id*. at 33, n.32, RJN251. If the District Court below were correct that there is no reasonable expectation of privacy in URLs, then the FISA Court would not have needed to place restrictions on the NSA's request for bulk collection of Internet communications.

d. ***Facebook's view***: Finally, Facebook has always taken the position that URLs can contain private and sensitive information. Indeed, Facebook even admitted during the class period that when URLs are packaged up as a referrer header and sent to Facebook, it could present privacy issues. As pled in the SAC, Facebook engineer Matt Jones wrote a blog post called "Protecting Privacy with Referrers." ER1205; ER648. He first noted that Facebook does truly want to track its users across the internet:

> Here at Facebook, we're all about understanding how people interact with our site – including how they end up here from across the vast expanse of the internet. We're not the only ones, though – most web sites want similar insights about the people who use them.
>
> Despite its tragic misspelling, the HTTP standard's "referrer" header sent by browsers gives websites the information they need to see how users found them, and how they explore the sites once there.

Id. Then under the heading "Referrers: not always welcome," Mr. Jones added:

> But sometimes referrers just don't belong – maybe there is sensitive information in a URL, or maybe a site just doesn't want its users' browsers telling others how they use the site. . . . ***Facebook is one site where referrers don't really belong*** . . .

Id. (emphasis added).

Facebook's concern about sensitive information in Internet communications continues today. Facebook participated in an amicus brief with fellow technology companies filed with the Supreme Court in a pending case called *Carpenter v. U.S.* RJN174. There, Facebook and the other amici make a compelling case for the public's reasonable expectation of privacy even in automatically generated Internet communications, inconsistent with the ruling of the District Court. Here are some samples from the amicus brief:

> Using [the Internet and Internet-connected devices] often involves transmitting highly personal information through the networks and applications of digital service providers. . . . Because the data that is transmitted can reveal a wealth of detail about people's personal lives, however, users of digital technologies reasonably expect to retain significant privacy in that data.

Amicus Brief at 10, RJN194. Likewise:

> Transmitting personal data to the companies that provide digital products and services is an unavoidable condition of using technologies that people find beneficial and useful, and foregoing the use of those technologies for many is not an option. . . . But that data can often reveal details about the user's personal life and activities and therefore can require Fourth Amendment protection.

Id. at 14, RJN198. And finally:

> users consider many types of collected electronic data to be private – particularly given the personal details that information can reveal – regardless of whether transmission to a third party has occurred behind the scenes in the creation or processing of that data.

Id. at 19, RJN203.

4. The District Court resolved questions of fact at the pleading stage and introduced new facts not appearing in (and contradicting) the complaints.

A "plaintiff's expectation of privacy must be reasonable." *Hernandez*, 47 Cal. 4th at 287. "This element rests on an examination of 'customs, practices, and physical settings surrounding particular activities . . . as well as the opportunity to be notified in advance and consent to the intrusion." *Id*. (internal citations omitted). The court "examines all of the surrounding circumstances, including the degree and setting of the intrusion and the intruder's motives and objectives." *Id*. at 295 (internal citations omitted). Naturally, this examination is intensely factual, and a "judge should be cautious before substituting his or her judgment for that of the community." *Opperman v. Path, Inc*., 205 F. Supp. 3d 1064, 1080 (N.D. Cal. 2016) ("*Opperman II*").

The Plaintiffs here pled a robust bundle of facts to support the generally accepted conclusion that Internet users have a reasonable expectation of privacy in the URLs constituting their aggregated web-browsing history especially when defendant Facebook represented that it would not track the data post-logout. The

California Superior Court has so held, and Plaintiffs provided a copy of the opinion with the SAC. ER896. The Third Circuit has similarly held, twice. When the FTC learned of Facebook's conduct, the Commission required Facebook to submit to 20 years of privacy audits, and the background and result of that investigation and consent was included with the SAC. ER1222. Discovery revealed that Facebook knew what it was doing was wrong and consistent with *Hernandez*, Plaintiffs offered proof of Facebook's "motives and objectives." ER1211. The SAC also noted that in Europe, multiple countries have similarly determined that non-consensual web tracking is a violation of reasonable expectations of privacy. ER1229-ER1234.

Facebook offered no examples to the contrary – it identified no courts or regulatory agencies that ever blessed its improper tracking. Instead, as noted by the District Court, Facebook introduced new evidence that users might be able to block tracking cookies – in essence, introducing a question of fact whether Plaintiffs could have taken additional steps to block Facebook's unlawful tracking. ER20-ER21. The core of the argument would then be, essentially, if you don't lock your door, you can't complain when the thief walks in. But Facebook's evidence offered in support of its 12(b)(6) argument appears nowhere in the SAC and the question of whether the "cookie blocking" would even be relevant was never tested in discovery. Besides, Facebook told its subscribers precisely how to avoid the tracking – ***simply log out before surfing the web***. It cannot be that California law requires Internet

users to employ yet a second redundant method to block cookies to protect their privacy just in case Facebook had secretly rendered the first method useless.

In any event, the District Court's consideration and resolution of Facebook's new factual defense on a 12(b)(6) motion is inappropriate. For example, even if discovery showed that a Facebook subscriber could have easily blocked Facebook tracking cookies during the class period, no record evidence shows that Plaintiffs or any average Internet user would even know what URLs and referrer headers are, or that cookies can include referrer headers and user-identifying information. Just last month, for example, in a closely watched case brought by the Belgian Commission for the Protection of Personal Privacy, the Court of First Instance in Brussels held that Facebook's internet tracking today continues to violate European privacy rights. *See generally* RJN2 (original Dutch language opinion); RJN87 (certified English translation). Although Facebook now accurately discloses its policies regarding tracking cookies, the Court found that "it is not evident from the Cookies Policy that Facebook also collects the "URL" (Internet address) of the webpage visited, in addition to the cookies, which nevertheless enable it to precisely track the browsing behavior on third-party websites." Opinion at 66, RJN152. Similarly, the Court held, "it is not clear to an average Internet user that Facebook systematically tracks his/her browsing behavior based on every visit to a website . . . outside of the Facebook service with which an interaction possibility exists." *Id.* If American

Internet users in 2010 and 2011 were equally ill-informed about the nature of cookies and how they enable web tracking, Facebook's evidence that subscribers have some ability to block cookies would be irrelevant.

Finally, the only authority cited by the District Court to support Facebook's defense actually supports the Plaintiffs. *See* ER20-ER21. In *In re Hulu Privacy Litig.*, No. 11-cv-3764-LB, 2014 WL 2758598 (N.D. Cal. June 17, 2014), the parties submitted expert evidence at class certification. *Id*. at *8. Defendant submitted an expert report claiming that Hulu users can "take simple steps to block data transmissions from their browsers to third parties." *Id*. This is the exact language quoted by the District Court – it is not the finding of any court, but instead is the disputed conclusion of an expert witness for Hulu, Peter Weitzman.

Importantly, the expert admitted several things: first, he did not test any of the "simple steps" on browsers that would have been used during the *Hulu* class period (a period that, coincidentally, starts on April 21, 2010, just one day before the class period here), and he was unable to testify whether the "simple steps" would have even worked in 2010 and 2011. *Id*. at *9. The expert even concluded that none of the cookie blockers he tested would have worked properly on Internet Explorer, the most popular browser at the time: Ghostery wasn't available for IE11, and on IE10, "[s]ome interactions with the pages caused the browser to freeze." *Id*. Adblock wasn't even mentioned by the expert, and the final blocker tested (Adblock Plus)

wasn't available for IE at all during the class period. *Id*. Finally, none of the cookie blockers tested on Apple's Safari browser actually blocked Facebook like buttons, *id*., the primary social plugin at issue in this case. The District Court therefore erred in accepting Facebook's new evidence and resolving the resulting factual dispute at this stage of the litigation.

B. Non-consensual secret tracking of web browsing history, when linked to user identity, is "highly offensive" and "sufficiently serious" to sustain actions for Invasion of Privacy and Intrusion upon Seclusion

1. The District Court resolved questions of fact at the pleading stage and introduced new facts not appearing in (and contradicting) the complaints.

Whether an invasion of privacy is "highly offensive" or "sufficiently serious" is an intensely factual question. Courts evaluate the "degree and setting" of the intrusion, and the "intruder's motives and objectives." *Hernandez*, 47 Cal. 4th at 295. The SAC thoroughly pled the degree and setting of the intrusion – it was wholesale, surreptitious tracking of millions of Internet users' intimate web browsing histories, aggregated and personally linked to their identities. ER1211-ER1220. With the benefit of discovery, the Plaintiffs were also able to plead Facebook's motives and objectives, ER1211, including intense interest from privacy advocates, Congress and the FTC. On less compelling facts (where the unauthorized tracking gathered anonymous data), the Third Circuit found that it should be up a jury to determine whether the intrusion was highly offensive or sufficiently serious.

Google Cookie Placement, 806 F.3d at 151-52; s*ee also Opperman v. Path, Inc.*, 87 F. Supp. 3d 1018, 1061 (N.D. Cal. 2014) ("O*pperman I*") (finding it relevant that defendant's actions were "closely scrutinized" by the FTC, Congress and the media, and holding that the "highly offensive" determination "is best left for a jury").

Here, at the pleading stage, the District Court found that no reasonable jury could find Facebook's unauthorized web tracking "highly offensive." ER21. The Court found, without any factual record, that Facebook's intrusion could have easily been blocked, *id*., going beyond the allegations in the SAC, and despite Facebook's tracking being so secret that the best minds in the industry (and the FTC) were shocked when it was revealed. ER1222. The District Court also introduced new facts from an unidentified source regarding integration of content and analytics tools from other third-party servers. ER21. The Court then concluded that these same tools "transmit to third parties the same data that Plaintiffs claim is highly sensitive." *Id*. That is incorrect. The SAC alleges facts unique to Facebook and alleges that the web tracking accomplished by Facebook's plugins is only possible by Facebook. ER1196-ER1197. Furthermore, Facebook is able to track web browsing on a personally-identifiable basis. Most importantly, only Facebook tracked its subscribers post-logout. The Plaintiffs do not allege that all web tracking is "highly offensive," just the tracking of logged-out subscribers without consent. The Court did not address whether any other third-party content provider ever attempted such

personally-identifiable tracking and whether any Court ever found such conduct to be "routine" or unobjectionable.

2. The District Court's ruling (if accepted by the Ninth Circuit) would create a circuit split on an important question of California law.

Similar to the question of whether Plaintiffs have a reasonable expectation of privacy in their web browsing histories, the Third Circuit has also ruled, applying California law, that Google's unauthorized web tracking – even anonymous tracking – could be deemed highly offensive because defendant Google obtained the data without consent and in violation of its terms of use:

> Whether or not data-based targeting is the internet's pole star, users are entitled to deny consent, and they are entitled to rely on the public promises of companies they deal with. Furthermore, Google's alleged conduct was broad, touching untold millions of internet users; it was surreptitious, surfacing only because of the independent research of [Stanford University researcher Jonathan] Mayer and the Wall Street Journal.

Google Cookie Placement, 806 F.3d at 151. Similarly, in *Nickelodeon*, a different panel of the Third Circuit, citing *Google Cookie Placement*, found that Viacom's unauthorized data collection could be deemed "highly offensive" under closely analogous New Jersey law because it violated Viacom's own terms of service. *Nickelodeon*, 827 F.3d at 294-95. Contrary to the Third Circuit's ruling, the District Court below, however, found nothing "highly offensive" about Facebook's conduct, calling it "routine." ER21. Collection of subscribers' most intimate web browsing data cannot be excused as "routine" when done without consent and contrary to the

company's own promises and representations. If the Ninth Circuit were to affirm the District Court on this point, therefore, it would create a circuit split.

3. The District Court relied on case law that has been overturned or is distinguishable on the facts.

The District Court relied on a District of New Jersey opinion in a closely analogous discussion of the New Jersey law of invasion of privacy and intrusion upon seclusion. ER21; *In re Nickelodeon Consumer Privacy Litig*., No. 12-cv-7829, 2014 WL 3012873, at *19 (D.N.J. July 2, 2014) (district court ruling that unauthorized collection of web browsing history not "offensive to the reasonable person"). But the Third Circuit reversed that ruling. *Nickelodeon*, 827 F.3d at 294-95. As noted above, the Third Circuit found that because the data collection was contrary to the defendant's own representations, defendant had created the reasonable expectation of privacy. Similarly, a "reasonable jury" could conclude that "collecting information using duplicitous tactics" is offensive or sufficiently serious. *Id*. at 295.

The District Court also relied on two readily distinguishable cases. ER21. In *Low*, the district court found no "highly offensive" conduct but defendant LinkedIn, unlike Facebook, lawfully had the data. LinkedIn shared the data on an anonymous basis with advertisers, unlike Facebook, which obtained the data and linked it to personal identity. The data at issue in *Low* was also limited to LinkedIn profiles observed by plaintiff, rather than, as here, a person's entire web browsing history.

Low, 2011 WL 5509848 at *1. In *In re Google, Inc. Privacy Policy Litig.*, 58 F. Supp. 3d 968, 988 (N.D. Cal. 2014), Google had also lawfully collected all of the user data at issue. There was no intrusion or unauthorized tracking; the only question was whether combining otherwise lawfully obtained data from multiple Google-owned platforms would be "highly offensive" and the court said no. *Id*. Even if this conclusion were correct, the facts are far removed from the case at bar.

4. The District Court improperly disregarded the ruling of the California Superior Court in the related action Ung v. Facebook.

As argued above, the District Court was bound to follow California law as interpreted by the court of California, and the decision of the California Superior Court in *Ung v. Facebook* is the only case on point to date. ER896. In addition to finding a reasonable expectation of privacy in personally-identifiable aggregated web browsing history as discussed above, the Superior Court also found Facebook's invasion of that privacy to be "sufficiently serious." ER901. Plaintiffs incorporate by reference their arguments above regarding whether the District Court was required to either follow the Superior Court or explain why the Superior Court incorrectly interpreted California law.[8]

[8] The Plaintiffs in *Ung v. Facebook* did not assert a claim for Intrusion upon Seclusion but the Superior Court's analysis of "serious invasion" applies with equal force to the analysis of the "highly offensive" prong of a claim for Intrusion upon Seclusion.

III. The District Court Erroneously Dismissed the Plaintiffs' claims under the Wiretap Act and the California Invasion of Privacy Act.

A. Under the Wiretap Act and Section 631 of California Invasion of Privacy Act, Facebook is not a "party to the communication" that Facebook caused to be copied and redirected to itself.

To state a claim under the Wiretap Act, a plaintiff must allege an intentional "interception" of the contents of an electronic communication without consent (or court authorization) through the use of a device. *See, e.g., In rePharmatrak, Inc. Privacy Litig*., 329 F.3d 9, 18 (1st Cir. 2003). By statutory definition, one who is a party to the communication cannot "intercept" it: "It shall not be unlawful . . . to intercept a wire, oral, or electronic communication where such person is a party to the communication." 18 U.S.C. § 2511(2)(d). Similarly, CIPA § 631 also defines "interception" to require a third-party. ER18.[9]

In its motion to dismiss the FAC, Facebook argued that it rendered itself a party to communications between Plaintiffs and first-party websites through its own computer code which commanded the Plaintiffs' web-browsers to send Facebook the data without the knowledge, consent, or any action of the Plaintiff. The District Court rejected Facebook's argument. ER41-ER42. Later, in dismissing the SAC

[9] CIPA § 632, unlike § 631, does not forbid "interception" but rather unauthorized "eavesdropping or recording," even by a party to the communication. As discussed in Subsection B below, it was therefore error for the District Court to apply the "party to the communication" defense to the § 632 claim.

alleging identical facts on this point, the District Court reversed course and accepted Facebook's argument. ER17-ER18. The District Court was correct the first time.

The Wiretap Act does not define "party to the communication." Therefore, this Court must give the term its ordinary meaning. *Joffe v. Google*, 729 F.3d 1262, 1268 (9th Cir. 2013). Here, no ordinary person would conclude that Facebook suddenly becomes a party to *each and every communication* exchanged between the Plaintiffs and the first-party websites they visit when Facebook secretly and unlawfully fails to delete tracking cookies. To so hold would give Facebook license to manufacture a statutory exemption to the Wiretap Act by improperly failing to delete cookies upon logout – and by extension, any interceptor could circumvent the Wiretap simply by writing code that forces a computer to transmit electronic communications to the interceptor. Such a result would be repugnant to the plain meaning and spirit of the Wiretap Act. *See In re iPhone Application Litig*., 844 F. Supp. 2d 1040, 1062 (N.D. Cal. 2012) ("The intended communication is between the users' iPhone and the Wi-fi and cell phone towers, and Plaintiffs appear to allege that Apple designed its operating system to intercept that communication and transmit the information to Apple's servers. Apple cannot manufacture a statutory exception through its own accused conduct").

Two different Circuit Courts of Appeals have refused to apply the "party to the communication" exception under similar circumstances. *See In rePharmatrak*,

Inc. Privacy Litig., 329 F.3d 9 (1st Cir. 2003) (Wiretap Act applies to the acquisition of data by cookie companies that track users on other websites); *U.S. v. Szymuszkiewicz*, 622 F.3d 701 (7th Cir. 2010) (Wiretap Act violation after defendant set up an email forwarding rule in victim's computer causing victim's computer to forwarded victim's emails to defendant). The Third Circuit, meanwhile, has rendered inconsistent rulings. *Cf. Google Cookie Placement*, 806 F.3d at 143 (Google became "a party to the conversation . . . by deceiving the plaintiffs' browsers into thinking the cookie-setting entity was a first-party website") *with U.S. v. Eady*, 648 F. App'x 118, 191 (3d Cir. 2016) ("party" under Wiretap Act "is a participant whose presence is known to the other parties contemporaneously with the communication").

Consistent with *In re iPhone*, *Pharmatrak*, *Szymuszkiewicz and Eady*, the District Court below properly rejected Facebook's "party to the communication" defense the first time. As the Plaintiffs alleged in the FAC, they were unaware that Facebook continued to intercept personally-identifiable communications with first-party websites following logout, ER925, ER952, ER954, ER956, and it is irrelevant that the tracking "involved communication with a Facebook server." ER42. The District Court properly noted that Facebook's characterization of the interception "is incomplete" because it failed to account for the fact that Plaintiffs were unaware of the communication. As the Third Circuit noted in *Eady*, this lack of awareness

renders the "party to the communication" exception inapplicable. When the District Court dismissed the SAC, it abandoned the "awareness" test and simply held that Facebook was a party to the communication because the Plaintiffs' browsers sent a copy of the communication. The District Court neither explained its about-face nor cited caselaw supporting this this reversal.

Importantly, Facebook now also implicitly supports the basis for the District Court's original conclusion. In the Tech. Cos. Amicus Brief that Facebook and others recently filed in the Supreme Court in *Carpenter v. U.S.*, the amicii note that using the "Internet and Internet-connected devices . . . often involves transmitting highly personal information through the networks and applications of digital service providers." RJN193-RJN194. Furthermore:

> In particular, the analog-era notion that transmission of data to a third party is necessarily "voluntary" conduct that precludes Fourth Amendment protection should not apply in a world where devices and applications constantly transmit data to third parties by dint of their mere operation.

RJN195. Similarly:

> Transmitting personal data to the companies that provide digital products and services is an unavoidable condition of using technologies that people find beneficial and useful, and forgoing the use of those technologies for many is not an option.

RJN197. While *Carpenter* involves Fourth Amendment issues and not the "party to the communication" exception specifically, the reasoning of amicii applies with equal force here to show Facebook is not a "party to the communication."[10]

B. Under Section 632 of the California Invasion of Privacy Act, the Plaintiffs pled an objectively reasonable expectation that their communications would not be recorded.

As discussed above, the District Court dismissed three claims based on the "party to the communication" defense: The Wiretap Act; CIPA § 631; and CIPA § 632. However, even if this Court were to affirm the defense, it only disposes of the Wiretap Act claim and the CIPA § 631 claim. *There is no "party to the communication" defense under CIPA § 632*. The reason is simple: while section 631 forbids third-parties from intercepting certain electronic communications to which they are not parties, section 632 forbids the recording of (or eavesdropping on) certain electronic communications. Even a party to the communication is forbidden to record it where any other party has "an objectively reasonable expectation that the conversation is not being overheard or recorded." *Flanagan v. Flanagan*, 27 Cal. 4th 766, 768 (2002). Even were this Court to find Facebook was a party to the communications triggered by its improper third-party cookies and social plugins, it was objectively reasonable, at minimum, for Plaintiffs to believe

[10] Appellants also note that a substantially similar issue is presented in *Winston Smith, et. al. v. Facebook*, Case No. 17-16206 (9th Cir.), a case currently pending before this Circuit in which briefing has concluded.

Facebook would not record the communications. The District Court failed to analyze the Section 631 and 632 claims separately, and the dismissal of the Plaintiffs' claims under Section 632 should be reversed.

IV. Under the Stored Communications Act, the Plaintiffs sufficiently pled that their communications with third-party websites are in "temporary storage incidental to transmission" at the time Facebook caused the communications to be copied and redirected to Facebook.

The SCA defines "electronic storage" as (A) "any temporary, intermediate storage of a[n] … electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an [ECS] for purposes of backup protection of such communication." 18 U.S.C. § 2510(17)(A),(B). Plaintiffs allege Facebook gained access to the content of communications in cookies and referrer URLs written to the Plaintiffs' browser-managed files in real time contemporaneously with the transmission in browser-managed files, including: (1) URL requests present in the toolbar while a user remains present at a particular webpage; and (2) browsing history maintained by the web-browser for purposes of back-up protection. ER1239.

The District Court found that the Plaintiffs' URL's were not in "storage" as defined in the SCA because they were not stored temporarily "incident to their transmission." ER19. But this conclusion is a factual determination contrary to the allegations in the SAC. As Plaintiffs alleged, the contents of their communications with first-party websites enter temporary storage in the toolbar "once a user hits

Enter or clicks on a link [and] the communication is in the process of being sent and received between the user and the first-party website." ER1239. The web-browser stores a copy of the user's URL requests in the toolbar for only so long as "the user remains present at a particular webpage." *Id*. When users send their next communication, the stored communication is removed from the toolbar. Browsing history is not the same thing as data stored temporarily in the tool bar.

More importantly, the Court ignored the second definition of storage under Subsection (17)(B) -- storage for "purposes of backup protection." As the Ninth Circuit held in the context of emails, backup protection can be for the user's benefit or convenience, and need not be incidental to the transmission of the communication. *Theofel v. Farey-Jones*, 359 F.3d 1066, 1075 (9th Cir. 2004). If a computer unexpectedly shuts down or a browser unexpectedly quits, upon re-start the browser will repopulate the toolbar with the prior URL – it is thus used for backup protection.

V. Personal computers can be "facilities" through with "electronic communication services" are provided, within the meaning of the Stored Communications Act.

The SCA defines "facility" as the conduits "through which an electronic communication service [ECS] is provided." 18 U.S.C. § 2701(a). An ECS is defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications." The District Court held that home computers are not "facilities" within the meaning of the SCA. ER19-ER20. While courts are split on

this question, *cf. Garcia v. City of Laredo, Tex.*, 702 F.3d 788 (5th Cir. 2012) *with U.S. v. Councilman*, 418 F.3d 67, 77 (1st Cir. 2005), Plaintiffs submit that the better view includes personal computing devices and web browsers. If this Court were to adopt the District Court's reasoning, it would remove from law enforcement and technology companies an important tool against hackers who target home computers and browsers rather than large corporate servers. For example, Microsoft routinely uses the SCA to challenge computer hackers who gain unauthorized access to Internet Explorer and its constituent files located on the personal computing devices of IE users. *See, e.g., Microsoft v. Does* 1-8, 14-cv-00811-LO-IDD, 2015 U.S. Dist. LEXIS 110145, at *21 (E.D. Va. July 20, 2015) ("Microsoft's … Windows operating system and Internet Explorer software are facilities through which electronic communication services are provided.").

Moreover, PATRIOT Act amendments to Title III of the ECPA (wiretap or pen register orders) support Plaintiffs. Section 2518(1)(b)(ii) of Title 28 of the U.S. Code requires an applicant to provide a "particular description of the nature and location of the ***facilities*** from which or the place where the communication is to be intercepted." Likewise, section 3123(b)(1)(A) requires that a pen register order include the "telephone line or other ***facility***" to which the order applies. Originally, the ECPA only referenced "telephone lines," but Congress added the term "facilities" to modernize the statute. As explained in H.R. 107-236 at 52-53, ER324,

"facilities" should be understood to include cell phones and Internet communication devices or account information. The House Report explained that "such functions are commonly performed today by software instead of physical mechanisms." *Id*. If Congress intended "facilities" in the ECPA to include cell phones, it is illogical to exclude home computers and browsers from the definition.

VI. Plaintiffs sufficiently pled claims for breach of contract and breach of the implied covenant of good faith and fair dealing under California law.

A. Facebook breached its contracts with subscribers

A breach of contract claim under California law requires Plaintiffs to allege that (1) they entered into a contract with Facebook, (2) they performed or were excused from performance under the contract, (3) Facebook breached the contract, and (4) Plaintiffs suffered damages from the breach. ER4 (citing *Oasis W. Realty, LLC. v. Goldman*, 51 Cal. 4th 811, 821 (2011)). The District Court found no breach.

As Plaintiffs alleged in the TAC, there are multiple contracts governing their relationship with Facebook. The first is the SRR. ER56 ("The agreement governing Facebook's relationship with subscribers starts with the 'Statements of Rights and Responsibilities' or 'SRR.'"). An explicit term of the SRR was a promise to disclose to subscribers how Facebook would collect user data. The very first paragraph of the SRR makes privacy a core value, stating: "Your privacy is very important to us." *Id*. The SRR then states that the Privacy is "important," informs users how Facebook "can collect and can use your content and information," "encourage[s] users to read

it, and explicitly hyperlinks to it." ER62. But the Privacy Policy never disclosed the post-logout tracking. Facebook thus breached its promise in the SRR to disclose its data collection practices.

Furthermore, the Privacy Policy is a separate agreement irrespective of whether incorporated by reference into the SRR. ER58 ("The Privacy Policy is an agreement."); ER57 ("Each of the Additional Documents is an agreement with terms agreed to by Facebook and subscribers."). The Privacy Policy also explicitly stated that any future owner of Facebook "will still have to honor" the "***promises***" and "***commitments***" made in the Policy. ER58 (emphasis added). Furthermore, by Facebook's terms, the contract renews each time subscribers access their account. In the December 22, 2010 Privacy Policy, for example, Facebook said that "[b]y using or accessing Facebook, you agree to our privacy practices outlined here." *Id.* Indeed, despite arguing to the contrary before the District Court, Facebook has recently argued before this Court in a different pending case that its Privacy Policy is a contract, finding it "remarkabl[e]" that "plaintiffs' brief does not mention that they agreed to the Data Policy and Cookie Use agreement when they signed up for the service." *See Appellee's Brief*, *Smith v. Facebook, Inc.*, No. 17-16206, ECF 24 at 3 (9th Cir. Dec. 18, 2017). The District Court thus erred in limiting its analysis to whether the Privacy Policy had been incorporated by reference into the SRR without also considering whether the Privacy Policy itself is a contract.

Finally, as detailed in the TAC, Facebook's Help Center was incorporated by reference into the Privacy Policy, by Facebook's own design. In the Help Center, Facebook clearly promised that its web tracking would be limited to logged-in subscribers. *See* ER58-ER59. So for example, in one Help Center page—"what information does Facebook receive about me when I visit a website with a Facebook social plugin?"—Facebook informed its users that it received only "technical information," when users surf the internet, failing to disclose that it would receive personally-identifiable information. ER63. In a later version of this same page, Facebook added "if you are logged into Facebook, we also see your user ID number and email address." That the Help Center pages are the third link in the contractual chain does not defeat their contractual status. *See Ruffu v. Cal. Phys. Serv.*, No. A094979, 2002 WL 1352449, at *5 (Cal. Ct. App. June 20, 2002). A contract "need not recite that it 'incorporates' another document, so long as it 'guide[s] the reader to the incorporated document." *Shaw v. Regents of Univ. of Cal.*, 58 Cal. App. 4th 44, 54 (1997). Here, the Privacy Policy linked to the Help Center pages and directed users to them, without exclusion, rendering it part of the contract.

B. Facebook breached the implied covenant of good faith and fair dealing.

Under California law, the covenant of good faith and fair dealing is implied in all contracts. *Racine & Laramie, Ltd. v. Dept. of Parks & Recreation*, 11 Cal App. 4th 1026, 1031-32 (Ct. App. 4th Dist. 1992). This is done to "prevent a contracting

party from engaging in conduct which (while not technically transgressing the express covenants) frustrates the other party's right to the benefits of the contract." *Id*. Even if this Court agreed that Facebook's contracts never expressly addressed post-logout tracking, such activity breached the covenant of good faith and fair dealing because it frustrated the limited license granted by users as to what tracking Facebook could do. Facebook's bargain with subscribers included an explicit duty to disclose "how we can collect and can use your content and information," ER62, and as alleged in the complaint, post-logout tracking was neither disclosed nor expected. ER70. A reasonable jury could find that Facebook's decision to knowingly and secretly track subscribers post-logout was a breach of the duty to act in good faith because it frustrated one the core and express principles of the Facebook SRR – to respect privacy. *See also Hicks v. E.T. Legg & Assocs*., 89 Cal. 4th 496, 509 (2001) (it is generally a "question of fact" whether the implied covenant has been breached).

CONCLUSION

The Plaintiffs-Appellants respectfully request that the Court reverse the Judgment of the District Court and remand for further proceedings.

Dated: March 26, 2018
New York, NY

Respectfully submitted,

KAPLAN FOX & KILSHEIMER LLP

/s/ David A. Straite
Frederic S. Fox
David A. Straite
Ralph E. Labaton
850 Third Avenue, 14th Floor
New York, NY 10022
Tel.: 212.687.1980
Fax: 212.687.7714

KAPLAN FOX & KILSHEIMER LLP
Laurence D. King
Mathew George
Mario M. Choi
350 Sansome Street, Suite 400
San Francisco, CA 94104
Tel: 415.772.4700
Fax: 415.772.4707

SILVERMAN THOMPSON SLUTKIN WHITE LLC
Stephen G. Grygiel
201 North Charles Street, 26th Floor
Baltimore, Maryland 21201
Tel.: (443) 909-7516
Fax: (410) 547-2432

CERTIFICATE OF COMPLIANCE

I certify that pursuant to Fed. R. App. P. 32(a)(7)(C) and Ninth Circuit Rule 32-1, Brief for Plaintiffs-Appellants is proportionately spaced, has a 14-point typeface of and contains 13,484 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii).

/s/ David A. Straite
David A. Straite

STATEMENT OF RELATED CASES

Plaintiffs-Appellants are unaware of any cases pending in this Court that are related to this appeal, as defined and required by Circuit Rule 28.2.6.

/s/ David Straite
David A. Straite

ADDENDUM

Pursuant to Federal Rule of Appellate Procedure 28(f)

ADDENDUM - TABLE OF CONTENTS

Title I of the Electronic Communications Privacy Act (the "Wiretap Act")

18 U.S.C. § 2510 *et seq*.

§2510. Definitions

As used in this chapter-

(1) "wire communication" means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce;

(2) "oral communication" means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication;

(3) "State" means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, and any territory or possession of the United States;

(4) "intercept" means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.

(5) "electronic, mechanical, or other device" means any device or apparatus which can be used to intercept a wire, oral, or electronic communication other than-

(a) any telephone or telegraph instrument, equipment or facility, or any component thereof, (i) furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business; or (ii) being used by a provider of wire or electronic communication service in the ordinary course of its business, or by an investigative or law enforcement officer in the ordinary course of his duties;

(b) a hearing aid or similar device being used to correct subnormal hearing to not better than normal;

(6) "person" means any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation;

(7) "Investigative or law enforcement officer" means any officer of the United States or of a State or political subdivision thereof, who is empowered by law to

conduct investigations of or to make arrests for offenses enumerated in this chapter, and any attorney authorized by law to prosecute or participate in the prosecution of such offenses;

(8) "contents", when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication;

(9) "Judge of competent jurisdiction" means-

(a) a judge of a United States district court or a United States court of appeals; and

(b) a judge of any court of general criminal jurisdiction of a State who is authorized by a statute of that State to enter orders authorizing interceptions of wire, oral, or electronic communications;

(10) "communication common carrier" has the meaning given that term in section 3 of the Communications Act of 1934;

(11) "aggrieved person" means a person who was a party to any intercepted wire, oral, or electronic communication or a person against whom the interception was directed;

(12) "electronic communication" means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectroznic or photooptical system that affects interstate or foreign commerce, but does not include-

(A) any wire or oral communication;

(B) any communication made through a tone-only paging device;

(C) any communication from a tracking device (as defined in section 3117 of this title); or

(D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds;

(13) "user" means any person or entity who-

(A) uses an electronic communication service; and

(B) is duly authorized by the provider of such service to engage in such use;

(14) "electronic communications system" means any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications;

(15) "electronic communication service" means any service which provides to users thereof the ability to send or receive wire or electronic communications;

(16) "readily accessible to the general public" means, with respect to a radio communication, that such communication is not-

(A) scrambled or encrypted;

(B) transmitted using modulation techniques whose essential parameters have been withheld from the public with the intention of preserving the privacy of such communication;

(C) carried on a subcarrier or other signal subsidiary to a radio transmission;

(D) transmitted over a communication system provided by a common carrier, unless the communication is a tone only paging system communication; or

(E) transmitted on frequencies allocated under part 25, subpart D, E, or F of part 74, or part 94 of the Rules of the Federal Communications Commission, unless, in the case of a communication transmitted on a frequency allocated under part 74 that is not exclusively allocated to broadcast auxiliary services, the communication is a two-way voice communication by radio;

(17) "electronic storage" means-

(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and

(B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication;

(18) "aural transfer" means a transfer containing the human voice at any point between and including the point of origin and the point of reception;

(19) "foreign intelligence information", for purposes of section 2517(6) of this title, means-

(A) information, whether or not concerning a United States person, that relates to the ability of the United States to protect against-

(i) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

(ii) sabotage or international terrorism by a foreign power or an agent of a foreign power; or

(iii) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or

(B) information, whether or not concerning a United States person, with respect to a foreign power or foreign territory that relates to-

(i) the national defense or the security of the United States; or

(ii) the conduct of the foreign affairs of the United States;

(20) "protected computer" has the meaning set forth in section 1030; and

(21) "computer trespasser"-

(A) means a person who accesses a protected computer without authorization and thus has no reasonable expectation of privacy in any communication transmitted to, through, or from the protected computer; and

(B) does not include a person known by the owner or operator of the protected computer to have an existing contractual relationship with the owner or operator of the protected computer for access to all or part of the protected computer.

§2511. Interception and disclosure of wire, oral, or electronic communications prohibited

(1) Except as otherwise specifically provided in this chapter any person who-

(a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;

(b) intentionally uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when-

(i) such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication; or

(ii) such device transmits communications by radio, or interferes with the transmission of such communication; or

(iii) such person knows, or has reason to know, that such device or any component thereof has been sent through the mail or transported in interstate or foreign commerce; or

(iv) such use or endeavor to use (A) takes place on the premises of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or (B) obtains or is for the purpose of obtaining information relating to the operations of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or

(v) such person acts in the District of Columbia, the Commonwealth of Puerto Rico, or any territory or possession of the United States;

(c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;

(d) intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection; or

(e)(i) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, intercepted by means authorized by sections 2511(2)(a)(ii), 2511(2)(b)–(c), 2511(2)(e), 2516, and 2518 of this chapter, (ii) knowing or having reason to know that the information was obtained through the interception of such a communication in connection with a criminal investigation, (iii) having obtained or received the information in connection with a criminal investigation, and (iv) with intent to improperly obstruct, impede, or interfere with a duly authorized criminal investigation,

shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).

(2)(a)(i) It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

(ii) Notwithstanding any other law, providers of wire or electronic communication service, their officers, employees, and agents, landlords, custodians, or other persons, are authorized to provide information, facilities, or technical assistance to persons authorized by law to intercept wire, oral, or electronic communications or to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, if such provider, its officers,

employees, or agents, landlord, custodian, or other specified person, has been provided with-

(A) a court order directing such assistance or a court order pursuant to section 704 of the Foreign Intelligence Surveillance Act of 1978 signed by the authorizing judge, or

(B) a certification in writing by a person specified in section 2518(7) of this title or the Attorney General of the United States that no warrant or court order is required by law, that all statutory requirements have been met, and that the specified assistance is required,

setting forth the period of time during which the provision of the information, facilities, or technical assistance is authorized and specifying the information, facilities, or technical assistance required. No provider of wire or electronic communication service, officer, employee, or agent thereof, or landlord, custodian, or other specified person shall disclose the existence of any interception or surveillance or the device used to accomplish the interception or surveillance with respect to which the person has been furnished a court order or certification under this chapter, except as may otherwise be required by legal process and then only after prior notification to the Attorney General or to the principal prosecuting attorney of a State or any political subdivision of a State, as may be appropriate. Any such disclosure, shall render such person liable for the civil damages provided for in section 2520. No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, or agents, landlord, custodian, or other specified person for providing information, facilities, or assistance in accordance with the terms of a court order, statutory authorization, or certification under this chapter.

(iii) If a certification under subparagraph (ii)(B) for assistance to obtain foreign intelligence information is based on statutory authority, the certification shall identify the specific statutory provision and shall certify that the statutory requirements have been met.

(b) It shall not be unlawful under this chapter for an officer, employee, or agent of the Federal Communications Commission, in the normal course of his employment and in discharge of the monitoring responsibilities exercised by the Commission in the enforcement of chapter 5 of title 47 of the United States Code, to intercept a wire or electronic communication, or oral communication transmitted by radio, or to disclose or use the information thereby obtained.

(c) It shall not be unlawful under this chapter for a person acting under color of law to intercept a wire, oral, or electronic communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception.

(d) It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.

(e) Notwithstanding any other provision of this title or section 705 or 706 of the Communications Act of 1934, it shall not be unlawful for an officer, employee, or agent of the United States in the normal course of his official duty to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, as authorized by that Act.

(f) Nothing contained in this chapter or chapter 121 or 206 of this title, or section 705 of the Communications Act of 1934, shall be deemed to affect the acquisition by the United States Government of foreign intelligence information from international or foreign communications, or foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic communications system, utilizing a means other than electronic surveillance as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, and procedures in this chapter or chapter 121 and the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which electronic surveillance, as defined in section 101 of such Act, and the interception of domestic wire, oral, and electronic communications may be conducted.

(g) It shall not be unlawful under this chapter or chapter 121 of this title for any person-

(i) to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public;

(ii) to intercept any radio communication which is transmitted-

(I) by any station for the use of the general public, or that relates to ships, aircraft, vehicles, or persons in distress;

(II) by any governmental, law enforcement, civil defense, private land mobile, or public safety communications system, including police and fire, readily accessible to the general public;

(III) by a station operating on an authorized frequency within the bands allocated to the amateur, citizens band, or general mobile radio services; or

(IV) by any marine or aeronautical communications system;

(iii) to engage in any conduct which-

(I) is prohibited by section 633 of the Communications Act of 1934; or

(II) is excepted from the application of section 705(a) of the Communications Act of 1934 by section 705(b) of that Act;

(iv) to intercept any wire or electronic communication the transmission of which is causing harmful interference to any lawfully operating station or consumer electronic equipment, to the extent necessary to identify the source of such interference; or

(v) for other users of the same frequency to intercept any radio communication made through a system that utilizes frequencies monitored by individuals engaged in the provision or the use of such system, if such communication is not scrambled or encrypted.

(h) It shall not be unlawful under this chapter-

(i) to use a pen register or a trap and trace device (as those terms are defined for the purposes of chapter 206 (relating to pen registers and trap and trace devices) of this title); or

(ii) for a provider of electronic communication service to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire or electronic communication, or a user of that service, from fraudulent, unlawful or abusive use of such service.

(i) It shall not be unlawful under this chapter for a person acting under color of law to intercept the wire or electronic communications of a computer trespasser transmitted to, through, or from the protected computer, if-

(I) the owner or operator of the protected computer authorizes the interception of the computer trespasser's communications on the protected computer;

(II) the person acting under color of law is lawfully engaged in an investigation;

(III) the person acting under color of law has reasonable grounds to believe that the contents of the computer trespasser's communications will be relevant to the investigation; and

(IV) such interception does not acquire communications other than those transmitted to or from the computer trespasser.

(3)(a) Except as provided in paragraph (b) of this subsection, a person or entity providing an electronic communication service to the public shall not intentionally

divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient.

(b) A person or entity providing electronic communication service to the public may divulge the contents of any such communication-

(i) as otherwise authorized in section 2511(2)(a) or 2517 of this title;

(ii) with the lawful consent of the originator or any addressee or intended recipient of such communication;

(iii) to a person employed or authorized, or whose facilities are used, to forward such communication to its destination; or

(iv) which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency.

(4)(a) Except as provided in paragraph (b) of this subsection or in subsection (5), whoever violates subsection (1) of this section shall be fined under this title or imprisoned not more than five years, or both.

(b) Conduct otherwise an offense under this subsection that consists of or relates to the interception of a satellite transmission that is not encrypted or scrambled and that is transmitted-

(i) to a broadcasting station for purposes of retransmission to the general public; or

(ii) as an audio subcarrier intended for redistribution to facilities open to the public, but not including data transmissions or telephone calls,

is not an offense under this subsection unless the conduct is for the purposes of direct or indirect commercial advantage or private financial gain.

(5)(a)(i) If the communication is-

(A) a private satellite video communication that is not scrambled or encrypted and the conduct in violation of this chapter is the private viewing of that communication and is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain; or

(B) a radio communication that is transmitted on frequencies allocated under subpart D of part 74 of the rules of the Federal Communications Commission that is not scrambled or encrypted and the conduct in violation of this chapter is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain,

then the person who engages in such conduct shall be subject to suit by the Federal Government in a court of competent jurisdiction.

(ii) In an action under this subsection-

(A) if the violation of this chapter is a first offense for the person under paragraph (a) of subsection (4) and such person has not been found liable in a civil action under section 2520 of this title, the Federal Government shall be entitled to appropriate injunctive relief; and

(B) if the violation of this chapter is a second or subsequent offense under paragraph (a) of subsection (4) or such person has been found liable in any prior civil action under section 2520, the person shall be subject to a mandatory $500 civil fine.

(b) The court may use any means within its authority to enforce an injunction issued under paragraph (ii)(A), and shall impose a civil fine of not less than $500 for each violation of such an injunction.

§2512. Manufacture, distribution, possession, and advertising of wire, oral, or electronic communication intercepting devices prohibited

(1) Except as otherwise specifically provided in this chapter, any person who intentionally-

(a) sends through the mail, or sends or carries in interstate or foreign commerce, any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications;

(b) manufactures, assembles, possesses, or sells any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications, and that such device or any component thereof has been or will be sent through the mail or transported in interstate or foreign commerce; or

(c) places in any newspaper, magazine, handbill, or other publication or disseminates by electronic means any advertisement of-

(i) any electronic, mechanical, or other device knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications; or

(ii) any other electronic, mechanical, or other device, where such advertisement promotes the use of such device for the purpose of the surreptitious interception of wire, oral, or electronic communications,

knowing the content of the advertisement and knowing or having reason to know that such advertisement will be sent through the mail or transported in interstate or foreign commerce,

shall be fined under this title or imprisoned not more than five years, or both.

(2) It shall not be unlawful under this section for-

(a) a provider of wire or electronic communication service or an officer, agent, or employee of, or a person under contract with, such a provider, in the normal course of the business of providing that wire or electronic communication service, or

(b) an officer, agent, or employee of, or a person under contract with, the United States, a State, or a political subdivision thereof, in the normal course of the activities of the United States, a State, or a political subdivision thereof,

to send through the mail, send or carry in interstate or foreign commerce, or manufacture, assemble, possess, or sell any electronic, mechanical, or other device knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications.

(3) It shall not be unlawful under this section to advertise for sale a device described in subsection (1) of this section if the advertisement is mailed, sent, or carried in interstate or foreign commerce solely to a domestic provider of wire or electronic communication service or to an agency of the United States, a State, or a political subdivision thereof which is duly authorized to use such device.

§2513. Confiscation of wire, oral, or electronic communication intercepting devices

Any electronic, mechanical, or other device used, sent, carried, manufactured, assembled, possessed, sold, or advertised in violation of section 2511 or section 2512 of this chapter may be seized and forfeited to the United States. All provisions of law relating to (1) the seizure, summary and judicial forfeiture, and condemnation of vessels, vehicles, merchandise, and baggage for violations of the customs laws contained in title 19 of the United States Code, (2) the disposition of such vessels, vehicles, merchandise, and baggage or the proceeds from the sale thereof, (3) the remission or mitigation of such forfeiture, (4) the compromise of claims, and (5) the award of compensation to informers in respect of such forfeitures, shall apply to seizures and forfeitures incurred, or alleged to have been incurred, under the provisions of this section, insofar as applicable and not inconsistent with the

provisions of this section; except that such duties as are imposed upon the collector of customs or any other person with respect to the seizure and forfeiture of vessels, vehicles, merchandise, and baggage under the provisions of the customs laws contained in title 19 of the United States Code shall be performed with respect to seizure and forfeiture of electronic, mechanical, or other intercepting devices under this section by such officers, agents, or other persons as may be authorized or designated for that purpose by the Attorney General.

§2515. Prohibition of use as evidence of intercepted wire or oral communications

Whenever any wire or oral communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof if the disclosure of that information would be in violation of this chapter.

§2516. Authorization for interception of wire, oral, or electronic communications

(1) The Attorney General, Deputy Attorney General, Associate Attorney General, or any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General or acting Deputy Assistant Attorney General in the Criminal Division or National Security Division specially designated by the Attorney General, may authorize an application to a Federal judge of competent jurisdiction for, and such judge may grant in conformity with section 2518 of this chapter an order authorizing or approving the interception of wire or oral communications by the Federal Bureau of Investigation, or a Federal agency having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of-

(a) any offense punishable by death or by imprisonment for more than one year under sections 2122 and 2274 through 2277 of title 42 of the United States Code (relating to the enforcement of the Atomic Energy Act of 1954), section 2284 of title 42 of the United States Code (relating to sabotage of nuclear facilities or fuel), or under the following chapters of this title: chapter 10 (relating to biological weapons), chapter 37 (relating to espionage), chapter 55 (relating to kidnapping), chapter 90 (relating to protection of trade secrets), chapter 105 (relating to sabotage), chapter 115 (relating to treason), chapter 102 (relating to riots), chapter 65 (relating to malicious mischief), chapter 111 (relating to destruction of vessels), or chapter 81 (relating to piracy);

(b) a violation of section 186 or section 501(c) of title 29, United States Code (dealing with restrictions on payments and loans to labor organizations), or any offense which involves murder, kidnapping, robbery, or extortion, and which is punishable under this title;

(c) any offense which is punishable under the following sections of this title: section 37 (relating to violence at international airports), section 43 (relating to animal enterprise terrorism), section 81 (arson within special maritime and territorial jurisdiction), section 201 (bribery of public officials and witnesses), section 215 (relating to bribery of bank officials), section 224 (bribery in sporting contests), subsection (d), (e), (f), (g), (h), or (i) of section 844 (unlawful use of explosives), section 1032 (relating to concealment of assets), section 1084 (transmission of wagering information), section 751 (relating to escape), section 832 (relating to nuclear and weapons of mass destruction threats), section 842 (relating to explosive materials), section 930 (relating to possession of weapons in Federal facilities), section 1014 (relating to loans and credit applications generally; renewals and discounts), section 1114 (relating to officers and employees of the United States), section 1116 (relating to protection of foreign officials), sections 1503, 1512, and 1513 (influencing or injuring an officer, juror, or witness generally), section 1510 (obstruction of criminal investigations), section 1511 (obstruction of State or local law enforcement), section 1581 (peonage), section 1584 (involuntary servitude), section 1589 (forced labor), section 1590 (trafficking with respect to peonage, slavery, involuntary servitude, or forced labor), section 1591 (sex trafficking of children by force, fraud, or coercion), section 1592 (unlawful conduct with respect to documents in furtherance of trafficking, peonage, slavery, involuntary servitude, or forced labor), section 1751 (Presidential and Presidential staff assassination, kidnapping, and assault), section 1951 (interference with commerce by threats or violence), section 1952 (interstate and foreign travel or transportation in aid of racketeering enterprises), section 1958 (relating to use of interstate commerce facilities in the commission of murder for hire), section 1959 (relating to violent crimes in aid of racketeering activity), section 1954 (offer, acceptance, or solicitation to influence operations of employee benefit plan), section 1955 (prohibition of business enterprises of gambling), section 1956 (laundering of monetary instruments), section 1957 (relating to engaging in monetary transactions in property derived from specified unlawful activity), section 659 (theft from interstate shipment), section 664 (embezzlement from pension and welfare funds), section 1343 (fraud by wire, radio, or television), section 1344 (relating to bank fraud), section 1992 (relating to terrorist attacks against mass transportation), sections 2251 and 2252 (sexual exploitation of children),

section 2251A (selling or buying of children), section 2252A (relating to material constituting or containing child pornography), section 1466A (relating to child obscenity), section 2260 (production of sexually explicit depictions of a minor for importation into the United States), sections 2421, 2422, 2423, and 2425 (relating to transportation for illegal sexual activity and related crimes), sections 2312, 2313, 2314, and 2315 (interstate transportation of stolen property), section 2321 (relating to trafficking in certain motor vehicles or motor vehicle parts), section 2340A (relating to torture), section 1203 (relating to hostage taking), section 1029 (relating to fraud and related activity in connection with access devices), section 3146 (relating to penalty for failure to appear), section 3521(b)(3) (relating to witness relocation and assistance), section 32 (relating to destruction of aircraft or aircraft facilities), section 38 (relating to aircraft parts fraud), section 1963 (violations with respect to racketeer influenced and corrupt organizations), section 115 (relating to threatening or retaliating against a Federal official), section 1341 (relating to mail fraud), a felony violation of section 1030 (relating to computer fraud and abuse), section 351 (violations with respect to congressional, Cabinet, or Supreme Court assassinations, kidnapping, and assault), section 831 (relating to prohibited transactions involving nuclear materials), section 33 (relating to destruction of motor vehicles or motor vehicle facilities), section 175 (relating to biological weapons), section 175c (relating to variola virus), section 956 (conspiracy to harm persons or property overseas), a felony violation of section 1028 (relating to production of false identification documentation), section 1425 (relating to the procurement of citizenship or nationalization unlawfully), section 1426 (relating to the reproduction of naturalization or citizenship papers), section 1427 (relating to the sale of naturalization or citizenship papers), section 1541 (relating to passport issuance without authority), section 1542 (relating to false statements in passport applications), section 1543 (relating to forgery or false use of passports), section 1544 (relating to misuse of passports), section 1546 (relating to fraud and misuse of visas, permits, and other documents), or section 555 (relating to construction or use of international border tunnels);

(d) any offense involving counterfeiting punishable under section 471, 472, or 473 of this title;

(e) any offense involving fraud connected with a case under title 11 or the manufacture, importation, receiving, concealment, buying, selling, or otherwise dealing in narcotic drugs, marihuana, or other dangerous drugs, punishable under any law of the United States;

(f) any offense including extortionate credit transactions under sections 892, 893, or 894 of this title;

(g) a violation of section 5322 of title 31, United States Code (dealing with the reporting of currency transactions), or section 5324 of title 31, United States Code (relating to structuring transactions to evade reporting requirement prohibited);

(h) any felony violation of sections 2511 and 2512 (relating to interception and disclosure of certain communications and to certain intercepting devices) of this title;

(i) any felony violation of chapter 71 (relating to obscenity) of this title;

(j) any violation of section 60123(b) (relating to destruction of a natural gas pipeline), section 46502 (relating to aircraft piracy), the second sentence of section 46504 (relating to assault on a flight crew with dangerous weapon), or section 46505(b)(3) or (c) (relating to explosive or incendiary devices, or endangerment of human life, by means of weapons on aircraft) of title 49;

(k) any criminal violation of section 2778 of title 22 (relating to the Arms Export Control Act);

(l) the location of any fugitive from justice from an offense described in this section;

(m) a violation of section 274, 277, or 278 of the Immigration and Nationality Act (8 U.S.C. 1324, 1327, or 1328) (relating to the smuggling of aliens);

(n) any felony violation of sections 922 and 924 of title 18, United States Code (relating to firearms);

(o) any violation of section 5861 of the Internal Revenue Code of 1986 (relating to firearms);

(p) a felony violation of section 1028 (relating to production of false identification documents), section 1542 (relating to false statements in passport applications), section 1546 (relating to fraud and misuse of visas, permits, and other documents), section 1028A (relating to aggravated identity theft) of this title or a violation of section 274, 277, or 278 of the Immigration and Nationality Act (relating to the smuggling of aliens); or

(q) any criminal violation of section 229 (relating to chemical weapons) or section 2332, 2332a, 2332b, 2332d, 2332f, 2332g, 2332h 2339, 2339A, 2339B, 2339C, or 2339D of this title (relating to terrorism);

(r) any criminal violation of section 1 (relating to illegal restraints of trade or commerce), 2 (relating to illegal monopolizing of trade or commerce), or 3 (relating to illegal restraints of trade or commerce in territories or the District of Columbia) of the Sherman Act (15 U.S.C. 1, 2, 3);

(s) any violation of section 670 (relating to theft of medical products); or

(t) any conspiracy to commit any offense described in any subparagraph of this paragraph.

(2) The principal prosecuting attorney of any State, or the principal prosecuting attorney of any political subdivision thereof, if such attorney is authorized by a statute of that State to make application to a State court judge of competent jurisdiction for an order authorizing or approving the interception of wire, oral, or electronic communications, may apply to such judge for, and such judge may grant in conformity with section 2518 of this chapter and with the applicable State statute an order authorizing, or approving the interception of wire, oral, or electronic communications by investigative or law enforcement officers having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of the commission of the offense of murder, kidnapping human trafficking, child sexual exploitation, child pornography production,, gambling, robbery, bribery, extortion, or dealing in narcotic drugs, marihuana or other dangerous drugs, or other crime dangerous to life, limb, or property, and punishable by imprisonment for more than one year, designated in any applicable State statute authorizing such interception, or any conspiracy to commit any of the foregoing offenses.

(3) Any attorney for the Government (as such term is defined for the purposes of the Federal Rules of Criminal Procedure) may authorize an application to a Federal judge of competent jurisdiction for, and such judge may grant, in conformity with section 2518 of this title, an order authorizing or approving the interception of electronic communications by an investigative or law enforcement officer having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of any Federal felony.

§2517. Authorization for disclosure and use of intercepted wire, oral, or electronic communications

(1) Any investigative or law enforcement officer who, by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents to another investigative or law enforcement officer to the extent that such disclosure is appropriate to the proper performance of the official duties of the officer making or receiving the disclosure.

(2) Any investigative or law enforcement officer who, by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication or evidence derived therefrom may use such contents to the extent such use is appropriate to the proper performance of his official duties.

(3) Any person who has received, by any means authorized by this chapter, any information concerning a wire, oral, or electronic communication, or evidence derived therefrom intercepted in accordance with the provisions of this chapter may disclose the contents of that communication or such derivative evidence while giving testimony under oath or affirmation in any proceeding held under the authority of the United States or of any State or political subdivision thereof.

(4) No otherwise privileged wire, oral, or electronic communication intercepted in accordance with, or in violation of, the provisions of this chapter shall lose its privileged character.

(5) When an investigative or law enforcement officer, while engaged in intercepting wire, oral, or electronic communications in the manner authorized herein, intercepts wire, oral, or electronic communications relating to offenses other than those specified in the order of authorization or approval, the contents thereof, and evidence derived therefrom, may be disclosed or used as provided in subsections (1) and (2) of this section. Such contents and any evidence derived therefrom may be used under subsection (3) of this section when authorized or approved by a judge of competent jurisdiction where such judge finds on subsequent application that the contents were otherwise intercepted in accordance with the provisions of this chapter. Such application shall be made as soon as practicable.

(6) Any investigative or law enforcement officer, or attorney for the Government, who by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents to any other Federal law enforcement, intelligence, protective, immigration, national defense, or national security official to the extent that such contents include foreign intelligence or counterintelligence (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 401a)),[1] or foreign intelligence information (as defined in subsection (19) of section 2510 of this title), to assist the official who is to receive that information in the performance of his official duties. Any Federal official who receives information pursuant to this provision may use that information only as necessary in the conduct of that person's official duties subject to any limitations on the unauthorized disclosure of such information.

(7) Any investigative or law enforcement officer, or other Federal official in carrying out official duties as such Federal official, who by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents or derivative evidence to a foreign investigative or law enforcement officer to the extent that such disclosure is appropriate to the proper performance of the official duties of the officer making or receiving the disclosure, and foreign investigative or law enforcement officers may use or disclose such contents or

derivative evidence to the extent such use or disclosure is appropriate to the proper performance of their official duties.

(8) Any investigative or law enforcement officer, or other Federal official in carrying out official duties as such Federal official, who by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents or derivative evidence to any appropriate Federal, State, local, or foreign government official to the extent that such contents or derivative evidence reveals a threat of actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power, domestic or international sabotage, domestic or international terrorism, or clandestine intelligence gathering activities by an intelligence service or network of a foreign power or by an agent of a foreign power, within the United States or elsewhere, for the purpose of preventing or responding to such a threat. Any official who receives information pursuant to this provision may use that information only as necessary in the conduct of that person's official duties subject to any limitations on the unauthorized disclosure of such information, and any State, local, or foreign official who receives information pursuant to this provision may use that information only consistent with such guidelines as the Attorney General and Director of Central Intelligence shall jointly issue.

§2518. Procedure for interception of wire, oral, or electronic communications

(1) Each application for an order authorizing or approving the interception of a wire, oral, or electronic communication under this chapter shall be made in writing upon oath or affirmation to a judge of competent jurisdiction and shall state the applicant's authority to make such application. Each application shall include the following information:

(a) the identity of the investigative or law enforcement officer making the application, and the officer authorizing the application;

(b) a full and complete statement of the facts and circumstances relied upon by the applicant, to justify his belief that an order should be issued, including (i) details as to the particular offense that has been, is being, or is about to be committed, (ii) except as provided in subsection (11), a particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted, (iii) a particular description of the type of communications sought to be intercepted, (iv) the identity of the person, if known, committing the offense and whose communications are to be intercepted;

(c) a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous;

(d) a statement of the period of time for which the interception is required to be maintained. If the nature of the investigation is such that the authorization for interception should not automatically terminate when the described type of communication has been first obtained, a particular description of facts establishing probable cause to believe that additional communications of the same type will occur thereafter;

(e) a full and complete statement of the facts concerning all previous applications known to the individual authorizing and making the application, made to any judge for authorization to intercept, or for approval of interceptions of, wire, oral, or electronic communications involving any of the same persons, facilities or places specified in the application, and the action taken by the judge on each such application; and

(f) where the application is for the extension of an order, a statement setting forth the results thus far obtained from the interception, or a reasonable explanation of the failure to obtain such results.

(2) The judge may require the applicant to furnish additional testimony or documentary evidence in support of the application.

(3) Upon such application the judge may enter an ex parte order, as requested or as modified, authorizing or approving interception of wire, oral, or electronic communications within the territorial jurisdiction of the court in which the judge is sitting (and outside that jurisdiction but within the United States in the case of a mobile interception device authorized by a Federal court within such jurisdiction), if the judge determines on the basis of the facts submitted by the applicant that-

(a) there is probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense enumerated in section 2516 of this chapter;

(b) there is probable cause for belief that particular communications concerning that offense will be obtained through such interception;

(c) normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous;

(d) except as provided in subsection (11), there is probable cause for belief that the facilities from which, or the place where, the wire, oral, or electronic communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such person.

(4) Each order authorizing or approving the interception of any wire, oral, or electronic communication under this chapter shall specify-

(a) the identity of the person, if known, whose communications are to be intercepted;

(b) the nature and location of the communications facilities as to which, or the place where, authority to intercept is granted;

(c) a particular description of the type of communication sought to be intercepted, and a statement of the particular offense to which it relates;

(d) the identity of the agency authorized to intercept the communications, and of the person authorizing the application; and

(e) the period of time during which such interception is authorized, including a statement as to whether or not the interception shall automatically terminate when the described communication has been first obtained.

An order authorizing the interception of a wire, oral, or electronic communication under this chapter shall, upon request of the applicant, direct that a provider of wire or electronic communication service, landlord, custodian or other person shall furnish the applicant forthwith all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference with the services that such service provider, landlord, custodian, or person is according the person whose communications are to be intercepted. Any provider of wire or electronic communication service, landlord, custodian or other person furnishing such facilities or technical assistance shall be compensated therefor by the applicant for reasonable expenses incurred in providing such facilities or assistance. Pursuant to section 2522 of this chapter, an order may also be issued to enforce the assistance capability and capacity requirements under the Communications Assistance for Law Enforcement Act.

(5) No order entered under this section may authorize or approve the interception of any wire, oral, or electronic communication for any period longer than is necessary to achieve the objective of the authorization, nor in any event longer than thirty days. Such thirty-day period begins on the earlier of the day on which the investigative or law enforcement officer first begins to conduct an interception under the order or ten days after the order is entered. Extensions of an order may be granted, but only upon application for an extension made in accordance with subsection (1) of this section and the court making the findings required by subsection (3) of this section. The period of extension shall be no longer than the authorizing judge deems necessary to achieve the purposes for which it was granted and in no event for longer than thirty days. Every order and extension thereof shall contain a provision that the authorization to intercept shall be executed as soon as practicable, shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter, and must terminate upon attainment of the authorized objective, or in any event in thirty days.

In the event the intercepted communication is in a code or foreign language, and an expert in that foreign language or code is not reasonably available during the interception period, minimization may be accomplished as soon as practicable after such interception. An interception under this chapter may be conducted in whole or in part by Government personnel, or by an individual operating under a contract with the Government, acting under the supervision of an investigative or law enforcement officer authorized to conduct the interception.

(6) Whenever an order authorizing interception is entered pursuant to this chapter, the order may require reports to be made to the judge who issued the order showing what progress has been made toward achievement of the authorized objective and the need for continued interception. Such reports shall be made at such intervals as the judge may require.

(7) Notwithstanding any other provision of this chapter, any investigative or law enforcement officer, specially designated by the Attorney General, the Deputy Attorney General, the Associate Attorney General, or by the principal prosecuting attorney of any State or subdivision thereof acting pursuant to a statute of that State, who reasonably determines that-

(a) an emergency situation exists that involves-

(i) immediate danger of death or serious physical injury to any person,

(ii) conspiratorial activities threatening the national security interest, or

(iii) conspiratorial activities characteristic of organized crime,

that requires a wire, oral, or electronic communication to be intercepted before an order authorizing such interception can, with due diligence, be obtained, and

(b) there are grounds upon which an order could be entered under this chapter to authorize such interception,

may intercept such wire, oral, or electronic communication if an application for an order approving the interception is made in accordance with this section within forty-eight hours after the interception has occurred, or begins to occur. In the absence of an order, such interception shall immediately terminate when the communication sought is obtained or when the application for the order is denied, whichever is earlier. In the event such application for approval is denied, or in any other case where the interception is terminated without an order having been issued, the contents of any wire, oral, or electronic communication intercepted shall be treated as having been obtained in violation of this chapter, and an inventory shall be served as provided for in subsection (d) of this section on the person named in the application.

(8)(a) The contents of any wire, oral, or electronic communication intercepted by any means authorized by this chapter shall, if possible, be recorded on tape or wire or other comparable device. The recording of the contents of any wire, oral, or electronic communication under this subsection shall be done in such a way as will protect the recording from editing or other alterations. Immediately upon the expiration of the period of the order, or extensions thereof, such recordings shall be made available to the judge issuing such order and sealed under his directions. Custody of the recordings shall be wherever the judge orders. They shall not be destroyed except upon an order of the issuing or denying judge and in any event shall be kept for ten years. Duplicate recordings may be made for use or disclosure pursuant to the provisions of subsections (1) and (2) of section 2517 of this chapter for investigations. The presence of the seal provided for by this subsection, or a satisfactory explanation for the absence thereof, shall be a prerequisite for the use or disclosure of the contents of any wire, oral, or electronic communication or evidence derived therefrom under subsection (3) of section 2517.

(b) Applications made and orders granted under this chapter shall be sealed by the judge. Custody of the applications and orders shall be wherever the judge directs. Such applications and orders shall be disclosed only upon a showing of good cause before a judge of competent jurisdiction and shall not be destroyed except on order of the issuing or denying judge, and in any event shall be kept for ten years.

(c) Any violation of the provisions of this subsection may be punished as contempt of the issuing or denying judge.

(d) Within a reasonable time but not later than ninety days after the filing of an application for an order of approval under section 2518(7)(b) which is denied or the termination of the period of an order or extensions thereof, the issuing or denying judge shall cause to be served, on the persons named in the order or the application, and such other parties to intercepted communications as the judge may determine in his discretion that is in the interest of justice, an inventory which shall include notice of-

(1) the fact of the entry of the order or the application;

(2) the date of the entry and the period of authorized, approved or disapproved interception, or the denial of the application; and

(3) the fact that during the period wire, oral, or electronic communications were or were not intercepted.

The judge, upon the filing of a motion, may in his discretion make available to such person or his counsel for inspection such portions of the intercepted communications, applications and orders as the judge determines to be in the interest of justice. On an ex parte showing of good cause to a judge of competent jurisdiction the serving of the inventory required by this subsection may be postponed.

(9) The contents of any wire, oral, or electronic communication intercepted pursuant to this chapter or evidence derived therefrom shall not be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in a Federal or State court unless each party, not less than ten days before the trial, hearing, or proceeding, has been furnished with a copy of the court order, and accompanying application, under which the interception was authorized or approved. This ten-day period may be waived by the judge if he finds that it was not possible to furnish the party with the above information ten days before the trial, hearing, or proceeding and that the party will not be prejudiced by the delay in receiving such information.

(10)(a) Any aggrieved person in any trial, hearing, or proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, may move to suppress the contents of any wire or oral communication intercepted pursuant to this chapter, or evidence derived therefrom, on the grounds that-

(i) the communication was unlawfully intercepted;

(ii) the order of authorization or approval under which it was intercepted is insufficient on its face; or

(iii) the interception was not made in conformity with the order of authorization or approval.

Such motion shall be made before the trial, hearing, or proceeding unless there was no opportunity to make such motion or the person was not aware of the grounds of the motion. If the motion is granted, the contents of the intercepted wire or oral communication, or evidence derived therefrom, shall be treated as having been obtained in violation of this chapter. The judge, upon the filing of such motion by the aggrieved person, may in his discretion make available to the aggrieved person or his counsel for inspection such portions of the intercepted communication or evidence derived therefrom as the judge determines to be in the interests of justice.

(b) In addition to any other right to appeal, the United States shall have the right to appeal from an order granting a motion to suppress made under paragraph (a) of this subsection, or the denial of an application for an order of approval, if the United States attorney shall certify to the judge or other official granting such motion or denying such application that the appeal is not taken for purposes of delay. Such appeal shall be taken within thirty days after the date the order was entered and shall be diligently prosecuted.

(c) The remedies and sanctions described in this chapter with respect to the interception of electronic communications are the only judicial remedies and sanctions for nonconstitutional violations of this chapter involving such communications.

(11) The requirements of subsections (1)(b)(ii) and (3)(d) of this section relating to the specification of the facilities from which, or the place where, the communication is to be intercepted do not apply if-

(a) in the case of an application with respect to the interception of an oral communication-

(i) the application is by a Federal investigative or law enforcement officer and is approved by the Attorney General, the Deputy Attorney General, the Associate Attorney General, an Assistant Attorney General, or an acting Assistant Attorney General;

(ii) the application contains a full and complete statement as to why such specification is not practical and identifies the person committing the offense and whose communications are to be intercepted; and

(iii) the judge finds that such specification is not practical; and

(b) in the case of an application with respect to a wire or electronic communication-

(i) the application is by a Federal investigative or law enforcement officer and is approved by the Attorney General, the Deputy Attorney General, the Associate Attorney General, an Assistant Attorney General, or an acting Assistant Attorney General;

(ii) the application identifies the person believed to be committing the offense and whose communications are to be intercepted and the applicant makes a showing that there is probable cause to believe that the person's actions could have the effect of thwarting interception from a specified facility;

(iii) the judge finds that such showing has been adequately made; and

(iv) the order authorizing or approving the interception is limited to interception only for such time as it is reasonable to presume that the person identified in the application is or was reasonably proximate to the instrument through which such communication will be or was transmitted.

(12) An interception of a communication under an order with respect to which the requirements of subsections (1)(b)(ii) and (3)(d) of this section do not apply by reason of subsection (11)(a) shall not begin until the place where the communication is to be intercepted is ascertained by the person implementing the interception order. A provider of wire or electronic communications service that has received an order as provided for in subsection (11)(b) may move the court to modify or quash the

order on the ground that its assistance with respect to the interception cannot be performed in a timely or reasonable fashion. The court, upon notice to the government, shall decide such a motion expeditiously.

§2519. Reports concerning intercepted wire, oral, or electronic communications

(1) In January of each year, any judge who has issued an order (or an extension thereof) under section 2518 that expired during the preceding year, or who has denied approval of an interception during that year, shall report to the Administrative Office of the United States Courts-

(a) the fact that an order or extension was applied for;

(b) the kind of order or extension applied for (including whether or not the order was an order with respect to which the requirements of sections 2518(1)(b)(ii) and 2518(3)(d) of this title did not apply by reason of section 2518(11) of this title);

(c) the fact that the order or extension was granted as applied for, was modified, or was denied;

(d) the period of interceptions authorized by the order, and the number and duration of any extensions of the order;

(e) the offense specified in the order or application, or extension of an order;

(f) the identity of the applying investigative or law enforcement officer and agency making the application and the person authorizing the application; and

(g) the nature of the facilities from which or the place where communications were to be intercepted.

(2) In March of each year the Attorney General, an Assistant Attorney General specially designated by the Attorney General, or the principal prosecuting attorney of a State, or the principal prosecuting attorney for any political subdivision of a State, shall report to the Administrative Office of the United States Courts-

(a) the information required by paragraphs (a) through (g) of subsection (1) of this section with respect to each application for an order or extension made during the preceding calendar year;

(b) a general description of the interceptions made under such order or extension, including (i) the approximate nature and frequency of incriminating communications intercepted, (ii) the approximate nature and frequency of other communications intercepted, (iii) the approximate number of persons whose communications were intercepted, (iv) the number of orders in which encryption was encountered and whether such encryption prevented law enforcement from obtaining the plain text of communications intercepted

pursuant to such order, and (v) the approximate nature, amount, and cost of the manpower and other resources used in the interceptions;

(c) the number of arrests resulting from interceptions made under such order or extension, and the offenses for which arrests were made;

(d) the number of trials resulting from such interceptions;

(e) the number of motions to suppress made with respect to such interceptions, and the number granted or denied;

(f) the number of convictions resulting from such interceptions and the offenses for which the convictions were obtained and a general assessment of the importance of the interceptions; and

(g) the information required by paragraphs (b) through (f) of this subsection with respect to orders or extensions obtained in a preceding calendar year.

(3) In June of each year the Director of the Administrative Office of the United States Courts shall transmit to the Congress a full and complete report concerning the number of applications for orders authorizing or approving the interception of wire, oral, or electronic communications pursuant to this chapter and the number of orders and extensions granted or denied pursuant to this chapter during the preceding calendar year. Such report shall include a summary and analysis of the data required to be filed with the Administrative Office by subsections (1) and (2) of this section. The Director of the Administrative Office of the United States Courts is authorized to issue binding regulations dealing with the content and form of the reports required to be filed by subsections (1) and (2) of this section.

§2520. Recovery of civil damages authorized

(a) In General.-Except as provided in section 2511(2)(a)(ii), any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter may in a civil action recover from the person or entity, other than the United States, which engaged in that violation such relief as may be appropriate.

(b) Relief.-In an action under this section, appropriate relief includes-

(1) such preliminary and other equitable or declaratory relief as may be appropriate;

(2) damages under subsection (c) and punitive damages in appropriate cases; and

(3) a reasonable attorney's fee and other litigation costs reasonably incurred.

(c) Computation of Damages.-(1) In an action under this section, if the conduct in violation of this chapter is the private viewing of a private satellite video communication that is not scrambled or encrypted or if the communication is a radio communication that is transmitted on frequencies allocated under subpart D of part 74 of the rules of the Federal Communications Commission that is not scrambled or encrypted and the conduct is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain, then the court shall assess damages as follows:

(A) If the person who engaged in that conduct has not previously been enjoined under section 2511(5) and has not been found liable in a prior civil action under this section, the court shall assess the greater of the sum of actual damages suffered by the plaintiff, or statutory damages of not less than $50 and not more than $500.

(B) If, on one prior occasion, the person who engaged in that conduct has been enjoined under section 2511(5) or has been found liable in a civil action under this section, the court shall assess the greater of the sum of actual damages suffered by the plaintiff, or statutory damages of not less than $100 and not more than $1000.

(2) In any other action under this section, the court may assess as damages whichever is the greater of-

(A) the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation; or

(B) statutory damages of whichever is the greater of $100 a day for each day of violation or $10,000.

(d) Defense.-A good faith reliance on-

(1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization;

(2) a request of an investigative or law enforcement officer under section 2518(7) of this title; or

(3) a good faith determination that section 2511(3) or 2511(2)(i) of this title permitted the conduct complained of;

is a complete defense against any civil or criminal action brought under this chapter or any other law.

(e) Limitation.-A civil action under this section may not be commenced later than two years after the date upon which the claimant first has a reasonable opportunity to discover the violation.

(f) Administrative Discipline.-If a court or appropriate department or agency determines that the United States or any of its departments or agencies has violated any provision of this chapter, and the court or appropriate department or agency finds that the circumstances surrounding the violation raise serious questions about whether or not an officer or employee of the United States acted willfully or intentionally with respect to the violation, the department or agency shall, upon receipt of a true and correct copy of the decision and findings of the court or appropriate department or agency promptly initiate a proceeding to determine whether disciplinary action against the officer or employee is warranted. If the head of the department or agency involved determines that disciplinary action is not warranted, he or she shall notify the Inspector General with jurisdiction over the department or agency concerned and shall provide the Inspector General with the reasons for such determination.

(g) Improper Disclosure Is Violation.-Any willful disclosure or use by an investigative or law enforcement officer or governmental entity of information beyond the extent permitted by section 2517 is a violation of this chapter for purposes of section 2520(a).

§2521. Injunction against illegal interception

Whenever it shall appear that any person is engaged or is about to engage in any act which constitutes or will constitute a felony violation of this chapter, the Attorney General may initiate a civil action in a district court of the United States to enjoin such violation. The court shall proceed as soon as practicable to the hearing and determination of such an action, and may, at any time before final determination, enter such a restraining order or prohibition, or take such other action, as is warranted to prevent a continuing and substantial injury to the United States or to any person or class of persons for whose protection the action is brought. A proceeding under this section is governed by the Federal Rules of Civil Procedure, except that, if an indictment has been returned against the respondent, discovery is governed by the Federal Rules of Criminal Procedure.

§2522. Enforcement of the Communications Assistance for Law Enforcement Act

(a) Enforcement by Court Issuing Surveillance Order.-If a court authorizing an interception under this chapter, a State statute, or the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) or authorizing use of a pen register or a trap and trace device under chapter 206 or a State statute finds that a telecommunications carrier has failed to comply with the requirements of the Communications Assistance for Law Enforcement Act, the court may, in accordance with section 108 of such Act, direct that the carrier comply forthwith and may direct

that a provider of support services to the carrier or the manufacturer of the carrier's transmission or switching equipment furnish forthwith modifications necessary for the carrier to comply.

(b) Enforcement Upon Application by Attorney General.-The Attorney General may, in a civil action in the appropriate United States district court, obtain an order, in accordance with section 108 of the Communications Assistance for Law Enforcement Act, directing that a telecommunications carrier, a manufacturer of telecommunications transmission or switching equipment, or a provider of telecommunications support services comply with such Act.

(c) Civil Penalty.-

(1) In general.-A court issuing an order under this section against a telecommunications carrier, a manufacturer of telecommunications transmission or switching equipment, or a provider of telecommunications support services may impose a civil penalty of up to $10,000 per day for each day in violation after the issuance of the order or after such future date as the court may specify.

(2) Considerations.-In determining whether to impose a civil penalty and in determining its amount, the court shall take into account-

(A) the nature, circumstances, and extent of the violation;

(B) the violator's ability to pay, the violator's good faith efforts to comply in a timely manner, any effect on the violator's ability to continue to do business, the degree of culpability, and the length of any delay in undertaking efforts to comply; and

(C) such other matters as justice may require.

(d) Definitions.-As used in this section, the terms defined in section 102 of the Communications Assistance for Law Enforcement Act have the meanings provided, respectively, in such section.

Title II of the Electronic Communications Privacy Act

(the "Stored Communications Act"), 18 U.S.C. § 2701 *et seq*.

§2701. Unlawful access to stored communications

(a) Offense.-Except as provided in subsection (c) of this section whoever-

(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or

(2) intentionally exceeds an authorization to access that facility;

and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.

(b) Punishment.-The punishment for an offense under subsection (a) of this section is-

(1) if the offense is committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain, or in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or any State-

(A) a fine under this title or imprisonment for not more than 5 years, or both, in the case of a first offense under this subparagraph; and

(B) a fine under this title or imprisonment for not more than 10 years, or both, for any subsequent offense under this subparagraph; and

(2) in any other case-

(A) a fine under this title or imprisonment for not more than 1 year or both, in the case of a first offense under this paragraph; and

(B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under this subparagraph that occurs after a conviction of another offense under this section.

(c) Exceptions.-Subsection (a) of this section does not apply with respect to conduct authorized-

(1) by the person or entity providing a wire or electronic communications service;

(2) by a user of that service with respect to a communication of or intended for that user; or

(3) in section 2703, 2704 or 2518 of this title.

§2702. Voluntary disclosure of customer communications or records

(a) Prohibitions.-Except as provided in subsection (b) or (c)-

(1) a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; and

(2) a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service-

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service;

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing; and

(3) a provider of remote computing service or electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by paragraph (1) or (2)) to any governmental entity.

(b) Exceptions for disclosure of communications.-A provider described in subsection (a) may divulge the contents of a communication-

(1) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient;

(2) as otherwise authorized in section 2517, 2511(2)(a), or 2703 of this title;

(3) with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;

(4) to a person employed or authorized or whose facilities are used to forward such communication to its destination;

(5) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;

(6) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 2258A;

(7) to a law enforcement agency-

(A) if the contents-

(i) were inadvertently obtained by the service provider; and

(ii) appear to pertain to the commission of a crime; or

(8) to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency.

(c) Exceptions for Disclosure of Customer Records.-A provider described in subsection (a) may divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a)(1) or (a)(2))-

(1) as otherwise authorized in section 2703;

(2) with the lawful consent of the customer or subscriber;

(3) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;

(4) to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency;

(5) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 2258A; or

(6) to any person other than a governmental entity.

(d) Reporting of Emergency Disclosures.-On an annual basis, the Attorney General shall submit to the Committee on the Judiciary of the House of Representatives and the Committee on the Judiciary of the Senate a report containing-

(1) the number of accounts from which the Department of Justice has received voluntary disclosures under subsection (b)(8);

(2) a summary of the basis for disclosure in those instances where-

(A) voluntary disclosures under subsection (b)(8) were made to the Department of Justice; and

(B) the investigation pertaining to those disclosures was closed without the filing of criminal charges; and

(3) the number of accounts from which the Department of Justice has received voluntary disclosures under subsection (c)(4).

§2703. Required disclosure of customer communications or records

(a) Contents of Wire or Electronic Communications in Electronic Storage.-A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

(b) Contents of Wire or Electronic Communications in a Remote Computing Service.-(1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection-

(A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction; or

(B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity-

(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or

(ii) obtains a court order for such disclosure under subsection (d) of this section;

except that delayed notice may be given pursuant to section 2705 of this title.

(2) Paragraph (1) is applicable with respect to any wire or electronic communication that is held or maintained on that service-

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to

access the contents of any such communications for purposes of providing any services other than storage or computer processing.

(c) Records Concerning Electronic Communication Service or Remote Computing Service.-(1) A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity-

(A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction;

(B) obtains a court order for such disclosure under subsection (d) of this section;

(C) has the consent of the subscriber or customer to such disclosure;

(D) submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud for the name, address, and place of business of a subscriber or customer of such provider, which subscriber or customer is engaged in telemarketing (as such term is defined in section 2325 of this title); or

(E) seeks information under paragraph (2).

(2) A provider of electronic communication service or remote computing service shall disclose to a governmental entity the-

(A) name;

(B) address;

(C) local and long distance telephone connection records, or records of session times and durations;

(D) length of service (including start date) and types of service utilized;

(E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and

(F) means and source of payment for such service (including any credit card or bank account number),

of a subscriber to or customer of such service when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under paragraph (1).

(3) A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer.

(d) Requirements for Court Order.-A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent

jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.

(e) No Cause of Action Against a Provider Disclosing Information Under This Chapter.-No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order, warrant, subpoena, statutory authorization, or certification under this chapter.

(f) Requirement To Preserve Evidence.-

(1) In general.-A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.

(2) Period of retention.-Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90-day period upon a renewed request by the governmental entity.

(g) Presence of Officer Not Required.-Notwithstanding section 3105 of this title, the presence of an officer shall not be required for service or execution of a search warrant issued in accordance with this chapter requiring disclosure by a provider of electronic communications service or remote computing service of the contents of communications or records or other information pertaining to a subscriber to or customer of such service.

§2704. Backup preservation

(a) Backup Preservation.-(1) A governmental entity acting under section 2703(b)(2) may include in its subpoena or court order a requirement that the service provider to whom the request is directed create a backup copy of the contents of the electronic communications sought in order to preserve those communications. Without notifying the subscriber or customer of such subpoena or court order, such service provider shall create such backup copy as soon as practicable consistent with its regular business practices and shall confirm to the governmental entity that such

backup copy has been made. Such backup copy shall be created within two business days after receipt by the service provider of the subpoena or court order.

(2) Notice to the subscriber or customer shall be made by the governmental entity within three days after receipt of such confirmation, unless such notice is delayed pursuant to section 2705(a).

(3) The service provider shall not destroy such backup copy until the later of-

(A) the delivery of the information; or

(B) the resolution of any proceedings (including appeals of any proceeding) concerning the government's subpoena or court order.

(4) The service provider shall release such backup copy to the requesting governmental entity no sooner than fourteen days after the governmental entity's notice to the subscriber or customer if such service provider-

(A) has not received notice from the subscriber or customer that the subscriber or customer has challenged the governmental entity's request; and

(B) has not initiated proceedings to challenge the request of the governmental entity.

(5) A governmental entity may seek to require the creation of a backup copy under subsection (a)(1) of this section if in its sole discretion such entity determines that there is reason to believe that notification under section 2703 of this title of the existence of the subpoena or court order may result in destruction of or tampering with evidence. This determination is not subject to challenge by the subscriber or customer or service provider.

(b) Customer Challenges.-(1) Within fourteen days after notice by the governmental entity to the subscriber or customer under subsection (a)(2) of this section, such subscriber or customer may file a motion to quash such subpoena or vacate such court order, with copies served upon the governmental entity and with written notice of such challenge to the service provider. A motion to vacate a court order shall be filed in the court which issued such order. A motion to quash a subpoena shall be filed in the appropriate United States district court or State court. Such motion or application shall contain an affidavit or sworn statement-

(A) stating that the applicant is a customer or subscriber to the service from which the contents of electronic communications maintained for him have been sought; and

(B) stating the applicant's reasons for believing that the records sought are not relevant to a legitimate law enforcement inquiry or that there has not been substantial compliance with the provisions of this chapter in some other respect.

(2) Service shall be made under this section upon a governmental entity by delivering or mailing by registered or certified mail a copy of the papers to the person, office, or department specified in the notice which the customer has received pursuant to this chapter. For the purposes of this section, the term "delivery" has the meaning given that term in the Federal Rules of Civil Procedure.

(3) If the court finds that the customer has complied with paragraphs (1) and (2) of this subsection, the court shall order the governmental entity to file a sworn response, which may be filed in camera if the governmental entity includes in its response the reasons which make in camera review appropriate. If the court is unable to determine the motion or application on the basis of the parties' initial allegations and response, the court may conduct such additional proceedings as it deems appropriate. All such proceedings shall be completed and the motion or application decided as soon as practicable after the filing of the governmental entity's response.

(4) If the court finds that the applicant is not the subscriber or customer for whom the communications sought by the governmental entity are maintained, or that there is a reason to believe that the law enforcement inquiry is legitimate and that the communications sought are relevant to that inquiry, it shall deny the motion or application and order such process enforced. If the court finds that the applicant is the subscriber or customer for whom the communications sought by the governmental entity are maintained, and that there is not a reason to believe that the communications sought are relevant to a legitimate law enforcement inquiry, or that there has not been substantial compliance with the provisions of this chapter, it shall order the process quashed.

(5) A court order denying a motion or application under this section shall not be deemed a final order and no interlocutory appeal may be taken therefrom by the customer.

§2705. Delayed notice

(a) Delay of Notification.-(1) A governmental entity acting under section 2703(b) of this title may-

(A) where a court order is sought, include in the application a request, which the court shall grant, for an order delaying the notification required under section 2703(b) of this title for a period not to exceed ninety days, if the court determines that there is reason to believe that notification of the existence of the court order may have an adverse result described in paragraph (2) of this subsection; or

(B) where an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury subpoena is obtained, delay the notification required under section 2703(b) of this title for a period not to exceed ninety days upon the execution of a written certification of a

supervisory official that there is reason to believe that notification of the existence of the subpoena may have an adverse result described in paragraph (2) of this subsection.

(2) An adverse result for the purposes of paragraph (1) of this subsection is-

(A) endangering the life or physical safety of an individual;

(B) flight from prosecution;

(C) destruction of or tampering with evidence;

(D) intimidation of potential witnesses; or

(E) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

(3) The governmental entity shall maintain a true copy of certification under paragraph (1)(B).

(4) Extensions of the delay of notification provided in section 2703 of up to ninety days each may be granted by the court upon application, or by certification by a governmental entity, but only in accordance with subsection (b) of this section.

(5) Upon expiration of the period of delay of notification under paragraph (1) or (4) of this subsection, the governmental entity shall serve upon, or deliver by registered or first-class mail to, the customer or subscriber a copy of the process or request together with notice that-

(A) states with reasonable specificity the nature of the law enforcement inquiry; and

(B) informs such customer or subscriber-

(i) that information maintained for such customer or subscriber by the service provider named in such process or request was supplied to or requested by that governmental authority and the date on which the supplying or request took place;

(ii) that notification of such customer or subscriber was delayed;

(iii) what governmental entity or court made the certification or determination pursuant to which that delay was made; and

(iv) which provision of this chapter allowed such delay.

(6) As used in this subsection, the term "supervisory official" means the investigative agent in charge or assistant investigative agent in charge or an equivalent of an investigating agency's headquarters or regional office, or the chief prosecuting attorney or the first assistant prosecuting attorney or an equivalent of a prosecuting attorney's headquarters or regional office.

(b) Preclusion of Notice to Subject of Governmental Access.-A governmental entity acting under section 2703, when it is not required to notify the subscriber or

customer under section 2703(b)(1), or to the extent that it may delay such notice pursuant to subsection (a) of this section, may apply to a court for an order commanding a provider of electronic communications service or remote computing service to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order. The court shall enter such an order if it determines that there is reason to believe that notification of the existence of the warrant, subpoena, or court order will result in-

(1) endangering the life or physical safety of an individual;

(2) flight from prosecution;

(3) destruction of or tampering with evidence;

(4) intimidation of potential witnesses; or

(5) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

§2706. Cost reimbursement

(a) Payment.-Except as otherwise provided in subsection (c), a governmental entity obtaining the contents of communications, records, or other information under section 2702, 2703, or 2704 of this title shall pay to the person or entity assembling or providing such information a fee for reimbursement for such costs as are reasonably necessary and which have been directly incurred in searching for, assembling, reproducing, or otherwise providing such information. Such reimbursable costs shall include any costs due to necessary disruption of normal operations of any electronic communication service or remote computing service in which such information may be stored.

(b) Amount.-The amount of the fee provided by subsection (a) shall be as mutually agreed by the governmental entity and the person or entity providing the information, or, in the absence of agreement, shall be as determined by the court which issued the order for production of such information (or the court before which a criminal prosecution relating to such information would be brought, if no court order was issued for production of the information).

(c) Exception.-The requirement of subsection (a) of this section does not apply with respect to records or other information maintained by a communications common carrier that relate to telephone toll records and telephone listings obtained under section 2703 of this title. The court may, however, order a payment as described in subsection (a) if the court determines the information required is unusually voluminous in nature or otherwise caused an undue burden on the provider.

§2707. Civil action

(a) Cause of Action.-Except as provided in section 2703(e), any provider of electronic communication service, subscriber, or other person aggrieved by any violation of this chapter in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind may, in a civil action, recover from the person or entity, other than the United States, which engaged in that violation such relief as may be appropriate.

(b) Relief.-In a civil action under this section, appropriate relief includes-

(1) such preliminary and other equitable or declaratory relief as may be appropriate;

(2) damages under subsection (c); and

(3) a reasonable attorney's fee and other litigation costs reasonably incurred.

(c) Damages.-The court may assess as damages in a civil action under this section the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation, but in no case shall a person entitled to recover receive less than the sum of $1,000. If the violation is willful or intentional, the court may assess punitive damages. In the case of a successful action to enforce liability under this section, the court may assess the costs of the action, together with reasonable attorney fees determined by the court.

(d) Administrative Discipline.-If a court or appropriate department or agency determines that the United States or any of its departments or agencies has violated any provision of this chapter, and the court or appropriate department or agency finds that the circumstances surrounding the violation raise serious questions about whether or not an officer or employee of the United States acted willfully or intentionally with respect to the violation, the department or agency shall, upon receipt of a true and correct copy of the decision and findings of the court or appropriate department or agency promptly initiate a proceeding to determine whether disciplinary action against the officer or employee is warranted. If the head of the department or agency involved determines that disciplinary action is not warranted, he or she shall notify the Inspector General with jurisdiction over the department or agency concerned and shall provide the Inspector General with the reasons for such determination.

(e) Defense.-A good faith reliance on-

(1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization (including a request of a governmental entity under section 2703(f) of this title);

(2) a request of an investigative or law enforcement officer under section 2518(7) of this title; or

(3) a good faith determination that section 2511(3) of this title permitted the conduct complained of;

is a complete defense to any civil or criminal action brought under this chapter or any other law.

(f) Limitation.-A civil action under this section may not be commenced later than two years after the date upon which the claimant first discovered or had a reasonable opportunity to discover the violation.

(g) Improper Disclosure.-Any willful disclosure of a "record", as that term is defined in section 552a(a) of title 5, United States Code, obtained by an investigative or law enforcement officer, or a governmental entity, pursuant to section 2703 of this title, or from a device installed pursuant to section 3123 or 3125 of this title, that is not a disclosure made in the proper performance of the official functions of the officer or governmental entity making the disclosure, is a violation of this chapter. This provision shall not apply to information previously lawfully disclosed (prior to the commencement of any civil or administrative proceeding under this chapter) to the public by a Federal, State, or local governmental entity or by the plaintiff in a civil action under this chapter.

§2708. Exclusivity of remedies

The remedies and sanctions described in this chapter are the only judicial remedies and sanctions for nonconstitutional violations of this chapter.

§2709. Counterintelligence access to telephone toll and transactional records

(a) Duty to Provide.-A wire or electronic communication service provider shall comply with a request for subscriber information and toll billing records information, or electronic communication transactional records in its custody or possession made by the Director of the Federal Bureau of Investigation under subsection (b) of this section.

(b) Required Certification.-The Director of the Federal Bureau of Investigation, or his designee in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge in a Bureau field office designated by the Director, may, using a term that specifically identifies a person, entity, telephone number, or account as the basis for a request-

(1) request the name, address, length of service, and local and long distance toll billing records of a person or entity if the Director (or his designee) certifies in writing to the wire or electronic communication service provider to which the request is made that the name, address, length of service, and toll billing records sought are relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities,

provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment to the Constitution of the United States; and

(2) request the name, address, and length of service of a person or entity if the Director (or his designee) certifies in writing to the wire or electronic communication service provider to which the request is made that the information sought is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution of the United States.

(c) Prohibition of Certain Disclosure.-

(1) Prohibition.-

(A) In general.-If a certification is issued under subparagraph (B) and notice of the right to judicial review under subsection (d) is provided, no wire or electronic communication service provider that receives a request under subsection (b), or officer, employee, or agent thereof, shall disclose to any person that the Federal Bureau of Investigation has sought or obtained access to information or records under this section.

(B) Certification.-The requirements of subparagraph (A) shall apply if the Director of the Federal Bureau of Investigation, or a designee of the Director whose rank shall be no lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge of a Bureau field office, certifies that the absence of a prohibition of disclosure under this subsection may result in-

(i) a danger to the national security of the United States;

(ii) interference with a criminal, counterterrorism, or counterintelligence investigation;

(iii) interference with diplomatic relations; or

(iv) danger to the life or physical safety of any person.

(2) Exception.-

(A) In general.-A wire or electronic communication service provider that receives a request under subsection (b), or officer, employee, or agent thereof, may disclose information otherwise subject to any applicable nondisclosure requirement to-

(i) those persons to whom disclosure is necessary in order to comply with the request;

(ii) an attorney in order to obtain legal advice or assistance regarding the request; or

(iii) other persons as permitted by the Director of the Federal Bureau of Investigation or the designee of the Director.

(B) Application.-A person to whom disclosure is made under subparagraph (A) shall be subject to the nondisclosure requirements applicable to a person to whom a request is issued under subsection (b) in the same manner as the person to whom the request is issued.

(C) Notice.-Any recipient that discloses to a person described in subparagraph (A) information otherwise subject to a nondisclosure requirement shall notify the person of the applicable nondisclosure requirement.

(D) Identification of disclosure recipients.-At the request of the Director of the Federal Bureau of Investigation or the designee of the Director, any person making or intending to make a disclosure under clause (i) or (iii) of subparagraph (A) shall identify to the Director or such designee the person to whom such disclosure will be made or to whom such disclosure was made prior to the request.

(d) Judicial Review.-

(1) In general.-A request under subsection (b) or a nondisclosure requirement imposed in connection with such request under subsection (c) shall be subject to judicial review under section 3511.

(2) Notice.-A request under subsection (b) shall include notice of the availability of judicial review described in paragraph (1).

(e) Dissemination by Bureau.-The Federal Bureau of Investigation may disseminate information and records obtained under this section only as provided in guidelines approved by the Attorney General for foreign intelligence collection and foreign counterintelligence investigations conducted by the Federal Bureau of Investigation, and, with respect to dissemination to an agency of the United States, only if such information is clearly relevant to the authorized responsibilities of such agency.

(f) Requirement That Certain Congressional Bodies Be Informed.-On a semiannual basis the Director of the Federal Bureau of Investigation shall fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate, and the Committee on the Judiciary of the House of Representatives and the Committee on

the Judiciary of the Senate, concerning all requests made under subsection (b) of this section.

(g) Libraries.-A library (as that term is defined in section 213(1) of the Library Services and Technology Act (20 U.S.C. 9122(1)), the services of which include access to the Internet, books, journals, magazines, newspapers, or other similar forms of communication in print or digitally by patrons for their use, review, examination, or circulation, is not a wire or electronic communication service provider for purposes of this section, unless the library is providing the services defined in section 2510(15) ("electronic communication service") of this title.

§2710. Wrongful disclosure of video tape rental or sale records

(a) Definitions.-For purposes of this section-

(1) the term "consumer" means any renter, purchaser, or subscriber of goods or services from a video tape service provider;

(2) the term "ordinary course of business" means only debt collection activities, order fulfillment, request processing, and the transfer of ownership;

(3) the term "personally identifiable information" includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider; and

(4) the term "video tape service provider" means any person, engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials, or any person or other entity to whom a disclosure is made under subparagraph (D) or (E) of subsection (b)(2), but only with respect to the information contained in the disclosure.

(b) Video Tape Rental and Sale Records.-(1) A video tape service provider who knowingly discloses, to any person, personally identifiable information concerning any consumer of such provider shall be liable to the aggrieved person for the relief provided in subsection (d).

(2) A video tape service provider may disclose personally identifiable information concerning any consumer-

(A) to the consumer;

(B) to any person with the informed, written consent (including through an electronic means using the Internet) of the consumer that-

(i) is in a form distinct and separate from any form setting forth other legal or financial obligations of the consumer;

(ii) at the election of the consumer-

(I) is given at the time the disclosure is sought; or

(II) is given in advance for a set period of time, not to exceed 2 years or until consent is withdrawn by the consumer, whichever is sooner; and

(iii) the video tape service provider has provided an opportunity, in a clear and conspicuous manner, for the consumer to withdraw on a case-by-case basis or to withdraw from ongoing disclosures, at the consumer's election;

(C) to a law enforcement agency pursuant to a warrant issued under the Federal Rules of Criminal Procedure, an equivalent State warrant, a grand jury subpoena, or a court order;

(D) to any person if the disclosure is solely of the names and addresses of consumers and if-

(i) the video tape service provider has provided the consumer with the opportunity, in a clear and conspicuous manner, to prohibit such disclosure; and

(ii) the disclosure does not identify the title, description, or subject matter of any video tapes or other audio visual material; however, the subject matter of such materials may be disclosed if the disclosure is for the exclusive use of marketing goods and services directly to the consumer;

(E) to any person if the disclosure is incident to the ordinary course of business of the video tape service provider; or

(F) pursuant to a court order, in a civil proceeding upon a showing of compelling need for the information that cannot be accommodated by any other means, if-

(i) the consumer is given reasonable notice, by the person seeking the disclosure, of the court proceeding relevant to the issuance of the court order; and

(ii) the consumer is afforded the opportunity to appear and contest the claim of the person seeking the disclosure.

If an order is granted pursuant to subparagraph (C) or (F), the court shall impose appropriate safeguards against unauthorized disclosure.

(3) Court orders authorizing disclosure under subparagraph (C) shall issue only with prior notice to the consumer and only if the law enforcement agency shows that there is probable cause to believe that the records or other information sought are relevant to a legitimate law enforcement inquiry. In the case of a State

government authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the video tape service provider, may quash or modify such order if the information or records requested are unreasonably voluminous in nature or if compliance with such order otherwise would cause an unreasonable burden on such provider.

(c) Civil Action.-(1) Any person aggrieved by any act of a person in violation of this section may bring a civil action in a United States district court.

(2) The court may award-

(A) actual damages but not less than liquidated damages in an amount of $2,500;

(B) punitive damages;

(C) reasonable attorneys' fees and other litigation costs reasonably incurred; and

(D) such other preliminary and equitable relief as the court determines to be appropriate.

(3) No action may be brought under this subsection unless such action is begun within 2 years from the date of the act complained of or the date of discovery.

(4) No liability shall result from lawful disclosure permitted by this section.

(d) Personally Identifiable Information.-Personally identifiable information obtained in any manner other than as provided in this section shall not be received in evidence in any trial, hearing, arbitration, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision of a State.

(e) Destruction of Old Records.-A person subject to this section shall destroy personally identifiable information as soon as practicable, but no later than one year from the date the information is no longer necessary for the purpose for which it was collected and there are no pending requests or orders for access to such information under subsection (b)(2) or (c)(2) or pursuant to a court order.

(f) Preemption.-The provisions of this section preempt only the provisions of State or local law that require disclosure prohibited by this section.

§2711. Definitions for chapter

As used in this chapter-

(1) the terms defined in section 2510 of this title have, respectively, the definitions given such terms in that section;

(2) the term "remote computing service" means the provision to the public of computer storage or processing services by means of an electronic communications system;

(3) the term "court of competent jurisdiction" includes-

(A) any district court of the United States (including a magistrate judge of such a court) or any United States court of appeals that-

(i) has jurisdiction over the offense being investigated;

(ii) is in or for a district in which the provider of a wire or electronic communication service is located or in which the wire or electronic communications, records, or other information are stored; or

(iii) is acting on a request for foreign assistance pursuant to section 3512 of this title; or

(B) a court of general criminal jurisdiction of a State authorized by the law of that State to issue search warrants; and

(4) the term "governmental entity" means a department or agency of the United States or any State or political subdivision thereof.

§2712. Civil actions against the United States

(a) In General.-Any person who is aggrieved by any willful violation of this chapter or of chapter 119 of this title or of sections 106(a), 305(a), or 405(a) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) may commence an action in United States District Court against the United States to recover money damages. In any such action, if a person who is aggrieved successfully establishes such a violation of this chapter or of chapter 119 of this title or of the above specific provisions of title 50, the Court may assess as damages-

(1) actual damages, but not less than $10,000, whichever amount is greater; and

(2) litigation costs, reasonably incurred.

(b) Procedures.-(1) Any action against the United States under this section may be commenced only after a claim is presented to the appropriate department or agency under the procedures of the Federal Tort Claims Act, as set forth in title 28, United States Code.

(2) Any action against the United States under this section shall be forever barred unless it is presented in writing to the appropriate Federal agency within 2 years after such claim accrues or unless action is begun within 6 months after the date of mailing, by certified or registered mail, of notice of final denial of the claim

by the agency to which it was presented. The claim shall accrue on the date upon which the claimant first has a reasonable opportunity to discover the violation.

(3) Any action under this section shall be tried to the court without a jury.

(4) Notwithstanding any other provision of law, the procedures set forth in section 106(f), 305(g), or 405(f) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) shall be the exclusive means by which materials governed by those sections may be reviewed.

(5) An amount equal to any award against the United States under this section shall be reimbursed by the department or agency concerned to the fund described in section 1304 of title 31, United States Code, out of any appropriation, fund, or other account (excluding any part of such appropriation, fund, or account that is available for the enforcement of any Federal law) that is available for the operating expenses of the department or agency concerned.

(c) Administrative Discipline.-If a court or appropriate department or agency determines that the United States or any of its departments or agencies has violated any provision of this chapter, and the court or appropriate department or agency finds that the circumstances surrounding the violation raise serious questions about whether or not an officer or employee of the United States acted willfully or intentionally with respect to the violation, the department or agency shall, upon receipt of a true and correct copy of the decision and findings of the court or appropriate department or agency promptly initiate a proceeding to determine whether disciplinary action against the officer or employee is warranted. If the head of the department or agency involved determines that disciplinary action is not warranted, he or she shall notify the Inspector General with jurisdiction over the department or agency concerned and shall provide the Inspector General with the reasons for such determination.

(d) Exclusive Remedy.-Any action against the United States under this subsection shall be the exclusive remedy against the United States for any claims within the purview of this section.

(e) Stay of Proceedings.-(1) Upon the motion of the United States, the court shall stay any action commenced under this section if the court determines that civil discovery will adversely affect the ability of the Government to conduct a related investigation or the prosecution of a related criminal case. Such a stay shall toll the limitations periods of paragraph (2) of subsection (b).

(2) In this subsection, the terms “related criminal case” and “related investigation” mean an actual prosecution or investigation in progress at the time at which the request for the stay or any subsequent motion to lift the stay is made. In determining whether an investigation or a criminal case is related to an action commenced under this section, the court shall consider the degree of similarity

between the parties, witnesses, facts, and circumstances involved in the 2 proceedings, without requiring that any one or more factors be identical.

(3) In requesting a stay under paragraph (1), the Government may, in appropriate cases, submit evidence ex parte in order to avoid disclosing any matter that may adversely affect a related investigation or a related criminal case. If the Government makes such an ex parte submission, the plaintiff shall be given an opportunity to make a submission to the court, not ex parte, and the court may, in its discretion, request further information from either party.

California Penal Code Sections 631 and 632

(the California Invasion of Privacy Act, or "CIPA")

631.

(a) Any person who, by means of any machine, instrument, or contrivance, or in any other manner, intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively, or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system, or who willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section, is punishable by a fine not exceeding two thousand five hundred dollars ($2,500), or by imprisonment in the county jail not exceeding one year, or by imprisonment pursuant to subdivision (h) of Section 1170, or by both a fine and imprisonment in the county jail or pursuant to subdivision (h) of Section 1170. If the person has previously been convicted of a violation of this section or Section 632, 632.5, 632.6, 632.7, or 636, he or she is punishable by a fine not exceeding ten thousand dollars ($10,000), or by imprisonment in the county jail not exceeding one year, or by imprisonment pursuant to subdivision (h) of Section 1170, or by both that fine and imprisonment.

(b) This section shall not apply (1) to any public utility engaged in the business of providing communications services and facilities, or to the officers, employees or agents thereof, where the acts otherwise prohibited herein are for the purpose of construction, maintenance, conduct or operation of the services and facilities of the public utility, or (2) to the use of any instrument, equipment, facility, or service furnished and used pursuant to the tariffs of a public utility, or (3) to any telephonic

communication system used for communication exclusively within a state, county, city and county, or city correctional facility.

(c) Except as proof in an action or prosecution for violation of this section, no evidence obtained in violation of this section shall be admissible in any judicial, administrative, legislative, or other proceeding.

(d) This section shall become operative on January 1, 1994.

(Amended by Stats. 2011, Ch. 15, Sec. 428. (AB 109) Effective April 4, 2011. Operative October 1, 2011, by Sec. 636 of Ch. 15, as amended by Stats. 2011, Ch. 39, Sec. 68.)

632.

(a) A person who, intentionally and without the consent of all parties to a confidential communication, uses an electronic amplifying or recording device to eavesdrop upon or record the confidential communication, whether the communication is carried on among the parties in the presence of one another or by means of a telegraph, telephone, or other device, except a radio, shall be punished by a fine not exceeding two thousand five hundred dollars ($2,500) per violation, or imprisonment in a county jail not exceeding one year, or in the state prison, or by both that fine and imprisonment. If the person has previously been convicted of a violation of this section or Section 631, 632.5, 632.6, 632.7, or 636, the person shall be punished by a fine not exceeding ten thousand dollars ($10,000) per violation, by imprisonment in a county jail not exceeding one year, or in the state prison, or by both that fine and imprisonment.

(b) For the purposes of this section, "person" means an individual, business association, partnership, corporation, limited liability company, or other legal entity, and an individual acting or purporting to act for or on behalf of any government or subdivision thereof, whether federal, state, or local, but excludes an individual known by all parties to a confidential communication to be overhearing or recording the communication.

(c) For the purposes of this section, "confidential communication" means any communication carried on in circumstances as may reasonably indicate that any party to the communication desires it to be confined to the parties thereto, but excludes a communication made in a public gathering or in any legislative, judicial, executive, or administrative proceeding open to the public, or in any other circumstance in which the parties to the communication may reasonably expect that the communication may be overheard or recorded.

(d) Except as proof in an action or prosecution for violation of this section, evidence obtained as a result of eavesdropping upon or recording a confidential communication in violation of this section is not admissible in any judicial, administrative, legislative, or other proceeding.

(e) This section does not apply (1) to any public utility engaged in the business of providing communications services and facilities, or to the officers, employees, or agents thereof, if the acts otherwise prohibited by this section are for the purpose of construction, maintenance, conduct, or operation of the services and facilities of the public utility, (2) to the use of any instrument, equipment, facility, or service furnished and used pursuant to the tariffs of a public utility, or (3) to any telephonic communication system used for communication exclusively within a state, county, city and county, or city correctional facility.

(f) This section does not apply to the use of hearing aids and similar devices, by persons afflicted with impaired hearing, for the purpose of overcoming the impairment to permit the hearing of sounds ordinarily audible to the human ear.

(Amended by Stats. 2016, Ch. 855, Sec. 1. (AB 1671) Effective January 1, 2017.)

California Penal Code Sections 484 (Statutory Larceny)

484.

(a) Every person who shall feloniously steal, take, carry, lead, or drive away the personal property of another, or who shall fraudulently appropriate property which has been entrusted to him or her, or who shall knowingly and designedly, by any false or fraudulent representation or pretense, defraud any other person of money, labor or real or personal property, or who causes or procures others to report falsely of his or her wealth or mercantile character and by thus imposing upon any person, obtains credit and thereby fraudulently gets or obtains possession of money, or property or obtains the labor or service of another, is guilty of theft. In determining the value of the property obtained, for the purposes of this section, the reasonable and fair market value shall be the test, and in determining the value of services received the contract price shall be the test. If there be no contract price, the reasonable and going wage for the service rendered shall govern. For the purposes of this section, any false or fraudulent representation or pretense made shall be treated as continuing, so as to cover any money, property or service received as a result thereof, and the complaint, information or indictment may charge that the crime was committed on any date during the particular period in question. The hiring of any additional employee or employees without advising each of them of every labor claim due and unpaid and every judgment that the employer has been unable to meet shall be prima facie evidence of intent to defraud.

(b) (1) Except as provided in Section 10855 of the Vehicle Code, where a person has leased or rented the personal property of another person pursuant to a written contract, and that property has a value greater than one thousand dollars ($1,000) and is not a commonly used household item, intent to commit theft by fraud shall be rebuttably presumed if the person fails to return the personal property to its owner within 10 days after the owner has made written demand by certified or registered mail following the expiration of the lease or rental agreement for return of the property so leased or rented.

(2) Except as provided in Section 10855 of the Vehicle Code, where a person has leased or rented the personal property of another person pursuant to a written

contract, and where the property has a value no greater than one thousand dollars ($1,000), or where the property is a commonly used household item, intent to commit theft by fraud shall be rebuttably presumed if the person fails to return the personal property to its owner within 20 days after the owner has made written demand by certified or registered mail following the expiration of the lease or rental agreement for return of the property so leased or rented.

(c) Notwithstanding the provisions of subdivision (b), if one presents with criminal intent identification which bears a false or fictitious name or address for the purpose of obtaining the lease or rental of the personal property of another, the presumption created herein shall apply upon the failure of the lessee to return the rental property at the expiration of the lease or rental agreement, and no written demand for the return of the leased or rented property shall be required.

(d) The presumptions created by subdivisions (b) and (c) are presumptions affecting the burden of producing evidence.

(e) Within 30 days after the lease or rental agreement has expired, the owner shall make written demand for return of the property so leased or rented. Notice addressed and mailed to the lessee or renter at the address given at the time of the making of the lease or rental agreement and to any other known address shall constitute proper demand. Where the owner fails to make such written demand the presumption created by subdivision (b) shall not apply.

(Amended by Stats. 2000, Ch. 176, Sec. 1. Effective January 1, 2001.)

California Penal Code Sections 496 (Statutory Larceny)

496.

(a) Every person who buys or receives any property that has been stolen or that has been obtained in any manner constituting theft or extortion, knowing the property to be so stolen or obtained, or who conceals, sells, withholds, or aids in concealing, selling, or withholding any property from the owner, knowing the property to be so stolen or obtained, shall be punished by imprisonment in a county jail for not more than one year, or imprisonment pursuant to subdivision (h) of Section 1170. However, if the value of the property does not exceed nine hundred fifty dollars ($950), the offense shall be a misdemeanor, punishable only by imprisonment in a county jail not exceeding one year, if such person has no prior convictions for an offense specified in clause (iv) of subparagraph (C) of paragraph (2) of subdivision (e) of Section 667 or for an offense requiring registration pursuant to subdivision (c) of Section 290.

A principal in the actual theft of the property may be convicted pursuant to this section. However, no person may be convicted both pursuant to this section and of the theft of the same property.

(b) Every swap meet vendor, as defined in Section 21661 of the Business and Professions Code, and every person whose principal business is dealing in, or collecting, merchandise or personal property, and every agent, employee, or representative of that person, who buys or receives any property of a value in excess of nine hundred fifty dollars ($950) that has been stolen or obtained in any manner constituting theft or extortion, under circumstances that should cause the person, agent, employee, or representative to make reasonable inquiry to ascertain that the person from whom the property was bought or received had the legal right to sell or deliver it, without making a reasonable inquiry, shall be punished by imprisonment in a county jail for not more than one year, or imprisonment pursuant to subdivision (h) of Section 1170.

Every swap meet vendor, as defined in Section 21661 of the Business and Professions Code, and every person whose principal business is dealing in, or collecting, merchandise or personal property, and every agent, employee, or representative of that person, who buys or receives any property of a value of nine hundred fifty dollars ($950) or less that has been stolen or obtained in any manner constituting theft or extortion, under circumstances that should cause the person, agent, employee, or representative to make reasonable inquiry to ascertain that the person from whom the property was bought or received had the legal right to sell or deliver it, without making a reasonable inquiry, shall be guilty of a misdemeanor.

(c) Any person who has been injured by a violation of subdivision (a) or (b) may bring an action for three times the amount of actual damages, if any, sustained by the plaintiff, costs of suit, and reasonable attorney's fees.

(d) Notwithstanding Section 664, any attempt to commit any act prohibited by this section, except an offense specified in the accusatory pleading as a misdemeanor, is punishable by imprisonment in a county jail for not more than one year, or by imprisonment pursuant to subdivision (h) of Section 1170.

(Amended November 4, 2014, by initiative Proposition 47, Sec. 9.)

California Penal Code Section 502

(Comprehensive Computer Data Access and Fraud Act, or "CDAFA")

502.

(a) It is the intent of the Legislature in enacting this section to expand the degree of protection afforded to individuals, businesses, and governmental agencies from tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems. The Legislature finds and declares that the proliferation of computer technology has resulted in a concomitant proliferation of computer crime and other forms of unauthorized access to computers, computer systems, and computer data.

The Legislature further finds and declares that protection of the integrity of all types and forms of lawfully created computers, computer systems, and computer data is vital to the protection of the privacy of individuals as well as to the well-being of financial institutions, business concerns, governmental agencies, and others within this state that lawfully utilize those computers, computer systems, and data.

(b) For the purposes of this section, the following terms have the following meanings:

(1) "Access" means to gain entry to, instruct, cause input to, cause output from, cause data processing with, or communicate with, the logical, arithmetical, or memory function resources of a computer, computer system, or computer network.

(2) "Computer network" means any system that provides communications between one or more computer systems and input/output devices, including, but not limited to, display terminals, remote systems, mobile devices, and printers connected by telecommunication facilities.

(3) "Computer program or software" means a set of instructions or statements, and related data, that when executed in actual or modified form, cause a computer, computer system, or computer network to perform specified functions.

(4) "Computer services" includes, but is not limited to, computer time, data processing, or storage functions, Internet services, electronic mail services, electronic message services, or other uses of a computer, computer system, or computer network.

(5) "Computer system" means a device or collection of devices, including support devices and excluding calculators that are not programmable and capable of being used in conjunction with external files, one or more of which contain computer programs, electronic instructions, input data, and output data, that performs functions, including, but not limited to, logic, arithmetic, data storage and retrieval, communication, and control.

(6) "Government computer system" means any computer system, or part thereof, that is owned, operated, or used by any federal, state, or local governmental entity.

(7) "Public safety infrastructure computer system" means any computer system, or part thereof, that is necessary for the health and safety of the public including computer systems owned, operated, or used by drinking water and wastewater treatment facilities, hospitals, emergency service providers, telecommunication companies, and gas and electric utility companies.

(8) "Data" means a representation of information, knowledge, facts, concepts, computer software, or computer programs or instructions. Data may be in any form, in storage media, or as stored in the memory of the computer or in transit or presented on a display device.

(9) "Supporting documentation" includes, but is not limited to, all information, in any form, pertaining to the design, construction, classification, implementation, use, or modification of a computer, computer system, computer network, computer program, or computer software, which information is not generally available to the public and is necessary for the operation of a computer, computer system, computer network, computer program, or computer software.

(10) "Injury" means any alteration, deletion, damage, or destruction of a computer system, computer network, computer program, or data caused by the access, or the denial of access to legitimate users of a computer system, network, or program.

(11) "Victim expenditure" means any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, or data was or was not altered, deleted, damaged, or destroyed by the access.

(12) "Computer contaminant" means any set of computer instructions that are designed to modify, damage, destroy, record, or transmit information within a computer, computer system, or computer network without the intent or permission of the owner of the information. They include, but are not limited to, a group of computer instructions commonly called viruses or worms, that are self-replicating or self-propagating and are designed to contaminate other computer programs or computer data, consume computer resources, modify, destroy, record, or transmit data, or in some other fashion usurp the normal operation of the computer, computer system, or computer network.

(13) "Internet domain name" means a globally unique, hierarchical reference to an Internet host or service, assigned through centralized Internet naming authorities, comprising a series of character strings separated by periods, with the rightmost character string specifying the top of the hierarchy.

(14) "Electronic mail" means an electronic message or computer file that is transmitted between two or more telecommunications devices; computers; computer networks, regardless of whether the network is a local, regional, or global network; or electronic devices capable of receiving electronic messages, regardless of whether the message is converted to hard copy format after receipt, viewed upon transmission, or stored for later retrieval.

(15) "Profile" means either of the following:

(A) A configuration of user data required by a computer so that the user may access programs or services and have the desired functionality on that computer.

(B) An Internet Web site user's personal page or section of a page that is made up of data, in text or graphical form, that displays significant, unique, or identifying information, including, but not limited to, listing acquaintances, interests, associations, activities, or personal statements.

(c) Except as provided in subdivision (h), any person who commits any of the following acts is guilty of a public offense:

(1) Knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data.

(2) Knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network.

(3) Knowingly and without permission uses or causes to be used computer services.

(4) Knowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network.

(5) Knowingly and without permission disrupts or causes the disruption of computer services or denies or causes the denial of computer services to an authorized user of a computer, computer system, or computer network.

(6) Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network in violation of this section.

(7) Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network.

(8) Knowingly introduces any computer contaminant into any computer, computer system, or computer network.

(9) Knowingly and without permission uses the Internet domain name or profile of another individual, corporation, or entity in connection with the sending of one or more electronic mail messages or posts and thereby damages or causes damage to a computer, computer data, computer system, or computer network.

(10) Knowingly and without permission disrupts or causes the disruption of government computer services or denies or causes the denial of government computer services to an authorized user of a government computer, computer system, or computer network.

(11) Knowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a public safety infrastructure computer system computer, computer system, or computer network.

(12) Knowingly and without permission disrupts or causes the disruption of public safety infrastructure computer system computer services or denies or causes the denial of computer services to an authorized user of a public safety infrastructure computer system computer, computer system, or computer network.

(13) Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or public safety infrastructure computer system computer, computer system, or computer network in violation of this section.

(14) Knowingly introduces any computer contaminant into any public safety infrastructure computer system computer, computer system, or computer network.

(d) (1) Any person who violates any of the provisions of paragraph (1), (2), (4), (5), (10), (11), or (12) of subdivision (c) is guilty of a felony, punishable by imprisonment pursuant to subdivision (h) of Section 1170 for 16 months, or two or three years and a fine not exceeding ten thousand dollars ($10,000), or a misdemeanor, punishable by imprisonment in a county jail not exceeding one year, by a fine not exceeding five thousand dollars ($5,000), or by both that fine and imprisonment.

(2) Any person who violates paragraph (3) of subdivision (c) is punishable as follows:

(A) For the first violation that does not result in injury, and where the value of the computer services used does not exceed nine hundred fifty dollars ($950), by a fine

not exceeding five thousand dollars ($5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment.

(B) For any violation that results in a victim expenditure in an amount greater than five thousand dollars ($5,000) or in an injury, or if the value of the computer services used exceeds nine hundred fifty dollars ($950), or for any second or subsequent violation, by a fine not exceeding ten thousand dollars ($10,000), or by imprisonment pursuant to subdivision (h) of Section 1170 for 16 months, or two or three years, or by both that fine and imprisonment, or by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment.

(3) Any person who violates paragraph (6), (7), or (13) of subdivision (c) is punishable as follows:

(A) For a first violation that does not result in injury, an infraction punishable by a fine not exceeding one thousand dollars ($1,000).

(B) For any violation that results in a victim expenditure in an amount not greater than five thousand dollars ($5,000), or for a second or subsequent violation, by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment.

(C) For any violation that results in a victim expenditure in an amount greater than five thousand dollars ($5,000), by a fine not exceeding ten thousand dollars ($10,000), or by imprisonment pursuant to subdivision (h) of Section 1170 for 16 months, or two or three years, or by both that fine and imprisonment, or by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment.

(4) Any person who violates paragraph (8) or (14) of subdivision (c) is punishable as follows:

(A) For a first violation that does not result in injury, a misdemeanor punishable by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment.

(B) For any violation that results in injury, or for a second or subsequent violation, by a fine not exceeding ten thousand dollars ($10,000), or by imprisonment in a county jail not exceeding one year, or by imprisonment pursuant to subdivision (h) of Section 1170, or by both that fine and imprisonment.

(5) Any person who violates paragraph (9) of subdivision (c) is punishable as follows:

(A) For a first violation that does not result in injury, an infraction punishable by a fine not exceeding one thousand dollars ($1,000).

(B) For any violation that results in injury, or for a second or subsequent violation, by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment.

(e) (1) In addition to any other civil remedy available, the owner or lessee of the computer, computer system, computer network, computer program, or data who suffers damage or loss by reason of a violation of any of the provisions of subdivision (c) may bring a civil action against the violator for compensatory damages and injunctive relief or other equitable relief. Compensatory damages shall include any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, or data was or was not altered, damaged, or deleted by the access. For the purposes of actions authorized by this subdivision, the conduct of an unemancipated minor shall be imputed to the

parent or legal guardian having control or custody of the minor, pursuant to the provisions of Section 1714.1 of the Civil Code.

(2) In any action brought pursuant to this subdivision the court may award reasonable attorney's fees.

(3) A community college, state university, or academic institution accredited in this state is required to include computer-related crimes as a specific violation of college or university student conduct policies and regulations that may subject a student to disciplinary sanctions up to and including dismissal from the academic institution. This paragraph shall not apply to the University of California unless the Board of Regents adopts a resolution to that effect.

(4) In any action brought pursuant to this subdivision for a willful violation of the provisions of subdivision (c), where it is proved by clear and convincing evidence that a defendant has been guilty of oppression, fraud, or malice as defined in subdivision (c) of Section 3294 of the Civil Code, the court may additionally award punitive or exemplary damages.

(5) No action may be brought pursuant to this subdivision unless it is initiated within three years of the date of the act complained of, or the date of the discovery of the damage, whichever is later.

(f) This section shall not be construed to preclude the applicability of any other provision of the criminal law of this state which applies or may apply to any transaction, nor shall it make illegal any employee labor relations activities that are within the scope and protection of state or federal labor laws.

(g) Any computer, computer system, computer network, or any software or data, owned by the defendant, that is used during the commission of any public offense described in subdivision (c) or any computer, owned by the defendant, which is used

as a repository for the storage of software or data illegally obtained in violation of subdivision (c) shall be subject to forfeiture, as specified in Section 502.01.

(h) (1) Subdivision (c) does not apply to punish any acts which are committed by a person within the scope of his or her lawful employment. For purposes of this section, a person acts within the scope of his or her employment when he or she performs acts which are reasonably necessary to the performance of his or her work assignment.

(2) Paragraph (3) of subdivision (c) does not apply to penalize any acts committed by a person acting outside of his or her lawful employment, provided that the employee's activities do not cause an injury, to the employer or another, or provided that the value of supplies or computer services which are used does not exceed an accumulated total of two hundred fifty dollars ($250).

(i) No activity exempted from prosecution under paragraph (2) of subdivision (h) which incidentally violates paragraph (2), (4), or (7) of subdivision (c) shall be prosecuted under those paragraphs.

(j) For purposes of bringing a civil or a criminal action under this section, a person who causes, by any means, the access of a computer, computer system, or computer network in one jurisdiction from another jurisdiction is deemed to have personally accessed the computer, computer system, or computer network in each jurisdiction.

(k) In determining the terms and conditions applicable to a person convicted of a violation of this section the court shall consider the following:

(1) The court shall consider prohibitions on access to and use of computers.

(2) Except as otherwise required by law, the court shall consider alternate sentencing, including community service, if the defendant shows remorse and recognition of the wrongdoing, and an inclination not to repeat the offense.

(Amended by Stats. 2015, Ch. 614, Sec. 1. (AB 32) Effective January 1, 2016.)

California Civil Code Sections 1572 and 1573 (Civil Fraud)

1572. Actual fraud, within the meaning of this Chapter, consists in any of the following acts, committed by a party to the contract, or with his connivance, with intent to deceive another party thereto, or to induce him to enter into the contract:

1. The suggestion, as a fact, of that which is not true, by one who does not believe it to be true;

2. The positive assertion, in a manner not warranted by the information of the person making it, of that which is not true, though he believes it to be true;

3. The suppression of that which is true, by one having knowledge or belief of the fact;

4. A promise made without any intention of performing it; or,

5. Any other act fitted to deceive.

1573. Constructive fraud consists:

1. In any breach of duty which, without an actually fraudulent intent, gains an advantage to the person in fault, or any one claiming under him, by misleading another to his prejudice, or to the prejudice of any one claiming under him; or,

2. In any such act or omission as the law specially declares to be fraudulent, without respect to actual fraud.

CERTIFICATE OF SERVICE

I hereby certify that on June 18, 2018, the I caused the foregoing BRIEF FOR PLAINTIFFS-APPELLANTS (FILED UNDER SEAL) to be sent by overnight delivery service to counsel of record for Defendant-Appellee Facebook, Inc.:

Lauren R. Goldman, Esq.
Michael Rayfield, Esq.
MAYER BROWN, LLP
1675 Broadway
New York, NY 10019-5820

Matthew D. Brown, Esq.
Jeffrey M. Gutkin, Esq.
Michael Graham Rhodes, Esq.
Kyle Christopher Wong, Esq.
COOLEY LLP
101 California Street, 5th Floor
San Francisco, CA 94111-5800

Additionally, I caused a courtesy PDF copy of the forgoing to be emailed to all counsel of record.

Dated: June 18, 2018

/s/ David Straite
David A. Straite