Public Version

No. 23-CV-550

IN THE DISTRICT OF COLUMBIA COURT OF APPEALS

DISTRICT OF COLUMBIA,
APPELLANT,

V.

FACEBOOK, INC.,
APPELLEE.

ON APPEAL FROM A JUDGMENT OF THE
SUPERIOR COURT OF THE DISTRICT OF COLUMBIA

CORRECTED REDACTED BRIEF FOR APPELLANT THE DISTRICT OF COLUMBIA

BRIAN L. SCHWALB
Attorney General for the District of Columbia

CAROLINE S. VAN ZILE
Solicitor General

ASHWIN P. PHATAK
Principal Deputy Solicitor General

GRAHAM E. PHILLIPS
Deputy Solicitor General

*JEREMY R. GIRTON
Assistant Attorney General
Office of the Solicitor General

Office of the Attorney General
400 6th Street, NW, Suite 8100
Washington, D.C. 20001
(202) 724-2029
jeremy.girton@dc.gov

*Counsel expected to argue

Public Version

TABLE OF CONTENTS

Public Version

TABLE OF AUTHORITIES*

Cases

---

* Authorities upon which we chiefly rely are marked with asterisks.

Statutes and Regulations

Other

Public Version

INTRODUCTION

This appeal stems from one of the largest data leaks in history. In March 2018, journalists revealed that Cambridge Analytica used personal data about tens of millions of Facebook users to influence the 2016 presidential election. The fallout from this news was enormous. Facebook took out full-page advertisements in newspapers around the world apologizing for the "breach of trust" and its failure to protect users' information. The company's stock value plunged by more than twenty percent. The Federal Trade Commission ultimately fined Facebook 5 billion dollars, one of the largest penalties ever assessed by the United States.

In truth, Facebook had known for years about the potential for this type of leak. Facebook opened up its social media network to third-party applications in 2007, allowing outside developers to siphon away a massive amount of personal data. Unbeknownst to most people, an application could collect a wealth of granular information not only about the users who downloaded the application, but also all of their friends, without those friends' knowledge or consent. By 2012, employees within Facebook had sounded the alarm that developers were receiving troves of data through this side door that could easily be misused or sold.

Despite knowing these risks, Facebook made many statements giving users the false impression that their information was private and within their control. It told users that it required third-party applications to respect their privacy, even

though Facebook devoted virtually no resources to oversight. It allowed users to customize their privacy settings, but it failed to explain that limiting sharing to "Friends Only" left their data open to third-party developers. And it suggested that data sharing required affirmative acts and consent, even though applications obtained data automatically. Facebook also failed to inform users of the Cambridge Analytica data leak for more than two years, until it became front-page news.

Because Facebook's privacy statements were materially misleading, the District sued Facebook for violating the Consumer Protection Procedures Act ("CPPA"), D.C. Code § 28-3901 *et seq.*, which prohibits unfair and deceptive trade practices in the District. The CPPA specifically bans companies from making misleading statements to their consumers or omitting material facts. In most CPPA cases, the central inquiry is whether the representations are likely to mislead a reasonable consumer. That question is ordinarily left to a jury.

Even though the District submitted ample evidence that Facebook misled and confused its customers about its data practices, the trial court perfunctorily dismissed the District's claims at summary judgment. It held that Facebook's statements could not be misleading as a matter of law because in a handful of isolated passages buried inside lengthy disclosures, Facebook hinted that friends could potentially "re-share" user information with third-party applications. This decision is wrong multiple times over. *First*, it blindly accepts the facts as presented by Facebook rather than viewing

contested facts in the light most favorable to the District, as the law requires. *Second*, it misconstrues the CPPA by allowing companies to escape liability for their misrepresentations by hiding truthful statements in places that consumers will never see. *Third*, it ignores important expert testimony showing that Facebook's privacy policies were unreadable and misleading to the average consumer.

STATEMENT OF THE ISSUES

1. Whether the Superior Court erred in granting summary judgment to Facebook on the District's consumer protection claim when there is a genuine factual dispute about whether Facebook's statements would mislead a reasonable consumer.

2. Whether the Superior Court abused its discretion when it excluded the District's expert, a recognized leader in the study of privacy notices who assessed Facebook's policies using widely accepted methods.

STATEMENT OF THE CASE

On December 19, 2018, the District sued Facebook for violating the CPPA.[1] JA 78-98. Facebook moved to dismiss for lack of personal jurisdiction and failure to state a claim and sought to stay the case pending other litigation. JA 4. The Superior Court denied that motion on May 31, 2019, and the case proceeded to discovery. JA 99-131. On May 17, 2022, Facebook moved for summary judgment

[1] In 2021, Facebook, Inc. changed its name to Meta Platforms, Inc. This brief continues to refer to the company as Facebook in line with the proceedings below.

and to exclude the District's expert, Dr. Florian Schaub. JA 142-84, 188-238. The Superior Court granted Facebook's motion to exclude on November 14, 2022, and it granted Facebook's motion for summary judgment on June 1, 2023. JA 961-62, 1029-46. The District timely appealed both rulings on June 29, 2023. JA 1047-52.

STATEMENT OF FACTS

1. Factual Background.

A. Facebook opens user data to third-party applications.

Facebook is the largest social media network in the world, with nearly [redacted] active users, including [redacted] users in the District of Columbia. JA 633, 668. Although Facebook allows users to share information, the company has long recognized—based on its own detailed studies—that users [redacted]. *See* JA 3991, 4000-06, 4074-75. Facebook acknowledged that the company would be successful only [redacted] JA 3693 (emphasis in original); *see Facebook, Social Media Privacy, and the Use and Abuse of Data*, S. Hrg. 115–683, 115th Cong. 135 (2018) [hereinafter "Senate"], *available at* https://cite.law/A5ZT-QNEG ("We know that if people don't trust that their information will be safe on Facebook, they won't feel comfortable using our services."). For that reason, Facebook emphasizes [redacted] to increase consumer trust. JA 3715. The perception that users have [redacted] over their information and can [redacted] has been vital to Facebook's success. JA 3063.

In 2007, Facebook launched Platform, a development space for third-party applications, like quizzes and games. JA 646-49. As part of Platform, Facebook created a mechanism known as "Graph API." JA 650. The original iteration of Graph API (version 1.0) allowed any third-party developer to create an application that could collect a [redacted] of information from Facebook. JA 4223. Critically, an application could access information not only about the user who downloaded the application, but also about every one of that user's *friends*, even if those friends had never heard of—much less downloaded—the application. JA 3212-14. This so-called "friend sharing" was not limited to friends' basic information. The interface allowed third parties to access twenty-nine data fields about users' friends, including date of birth, current city, hometown, relationship status, educational and work history, religious and political affiliations, and interests. JA 3212-14. It also provided access to all of the friend's activities on Facebook, including preferences about news, books, music, events, fitness, games, notes, photos, and videos. JA 3212-14.

Facebook exercised little oversight over what information third-party applications could access. Although Graph API version 1.0 launched in May 2007, Facebook did not even begin to have a process for vetting applications to determine whether the developer needed the data it was collecting until April 2014. JA 4172. During that initial seven-year period, an application developer [redacted]

[redacted] JA 4493.

B. Facebook's privacy disclosures and settings made it difficult for users to understand or control what data was available to third parties.

Although the ability of third-party applications to access friend data through Graph API version 1.0 was well known to Facebook, it was not readily understood by Facebook's users. During the relevant time, Facebook's disclosures about controlling third-party behavior were spread out over three different policy documents: the Statement of Rights and Responsibilities ("SRR," now known as the Terms of Service), the Data Use Policy, and the Platform Policy. *See* JA 2186-2488. These documents were lengthy and difficult to understand. For an average reader, it would have taken around an hour just to read them. JA 1538-40. Actually understanding the documents required first-year college reading comprehension, which is more advanced than what the average Facebook user possesses. JA 1537.

Facebook users specifically looking for information on what data third-party applications could access were also unlikely to find clear answers. For instance, the Data Use Policy in effect from 2012 through early 2015 acknowledged that information shared with friends could be "re-shared," but it implied that this sharing required an affirmative act by either the user or the user's friend:

> Just like when you share information by email or elsewhere on the web, information you share on Facebook can be re-shared. This means that

> if you share something on Facebook, anyone who can see it can share it with others, including the games, applications, and websites they use.

JA 2220, 2236. But a user did not need to actively "share" information with a friend—and the friend did not need to actively "re-share" it—for it to be available to application developers. When a user logged into a third-party application using Graph API version 1.0, the application received all of their friends' data "by default." JA 3064. Users of an application had no way to restrict what data the application would collect about their friends; they were forced to accept all permissions that an application requested or not use the application at all. JA 4224-25. Moreover, the Data Use Policy talked about "games, applications, and websites you *and* your friends use," implying that the use must be mutual, which was not the case. JA 2214, 2230 (emphasis added); *see* JA 2246 (discussing information shared "when you play a game with your Facebook friends").

Users seeking to control who could access their information had to navigate a maze of confusing and conflicting privacy settings. Between 2010 and 2012, a user who wanted to restrict access to their profile information would likely navigate to the "Profile Information" section of the privacy settings, where they could limit access to various categories of information to "Friends Only." JA 1525-26. But doing so would not have *actually* limited this information to the user's friends, because it would still be accessible to those friends' applications. Even after

Facebook redesigned its privacy settings in 2012, accessing "Privacy Settings and Tools" still did not warn users about applications or friend sharing. JA 429.

To change what information was accessible to applications, the user had to go to "Application Settings." JA 429. Even that page was deceiving. It showed a list of what applications the user had downloaded, but it did not show applications used by their friends. *See* JA 278, 2516. Similarly, pages like "Privacy Shortcuts," "Privacy Checkup," and "Privacy Basics" focused exclusively on the user's posts; they said nothing about personal information accessible to applications downloaded by the user's friends. *See* JA 2508-12. The only way for a user to prevent their data from being accessed by their friends' applications was to "turn off Platform" completely. JA 4173. Facebook strongly disincentivized users from taking this step with warnings such as, "But remember, you will not be able to use any games or apps yourself." JA 1558, 2524.

Even if a user read all of the relevant privacy policies and settings, the user would have encountered many statements giving the impression that Facebook had a robust system for protecting data. The SRR, for instance, stated, "We require applications to respect your privacy." *E.g.*, JA 2187. The Platform Policy listed specific terms for third-party developers, conveying restrictions and limitations on what third parties could do with user data. JA 2256-58. These included requirements to give users "control," to "protect data," and to "follow the law." *E.g.*,

JA 2256, 2264-65. The Data Use Policy assured users that if "an application asks permission from someone else to access your information, the application will be allowed to use that information only in connection with the person that gave the permission, no one else." JA 2220. The SRR also listed a variety of enforcement and oversight rights Facebook maintained over third-party applications, including Facebook's right to "analyze [the] app, content, and data for any purpose" and to "audit" it "[t]o ensure [the] application is safe for users." JA 2189-90.

Contrary to these assurances, [redacted]. JA 4494-95; *see* JA 4989-91. At least prior to [redacted], Facebook *never* [redacted]. JA 4505-06. And the number of third-party applications on Facebook was enormous—41 million in 2013—making it "practically impossible for Facebook to monitor individual compliance on a per-app basis." JA 804. [redacted] JA 4755.

Despite knowing these risks, Facebook devoted barely any resources to enforcement. Between 2011 and 2012, Facebook assigned only one person to

enforce its data policies on the millions of third-party applications. JA 4496-97. By 2014, the enforcement group had grown, but was still only [redacted]. JA 4910, 4919. In Facebook's own words, its enforcement of Platform policies was [redacted] JA 4462-66.

Even when Facebook became aware of violations, it often [redacted]. *E.g.*, JA 4517-18, 4521, 4556, 4667-69, 4689-94. Facebook would not [redacted] to a violation if it was not [redacted], JA 4530, 4999, or if the application had a sufficiently large [redacted] on Facebook, JA 4693. Facebook also [redacted] *See* JA 5091-96. Even when made aware that a whitelisted application was [redacted]. JA 5098-5102.

[redacted]. *E.g.*, JA 3972-73, 4048-71, 4088-97, 4101. For instance, Facebook acknowledged in a 2014 internal presentation that users have [redacted], and that the sharing is done [redacted]

[redacted] JA 4095. It also knew that its policies were [redacted]. JA 4464. Facebook conducted several studies and surveys showing that users [redacted]. JA 3998-4022. Nonetheless, users found it [redacted] privacy settings and were [redacted] about the permissions for third-party applications. JA 4020-29, 4044-71, 4074-75, 4077-81, 4107, 4176. The "report an app" function, for example, was [redacted] JA 3984, 5026-27.

C. Cambridge Analytica misuses data from millions of Facebook users.

Launching Platform proved incredibly lucrative for both Facebook and outside developers. Facebook gained millions of new applications, greatly enhancing the value of its social media service. Developers gained access to a wealth of information about users that could be readily monetized. As one Facebook employee explained, [redacted] JA 4501. [redacted]. JA 4696-4704. Facebook even allowed advertisers to target specific Facebook users based on demographics, interests, and behaviors—in other words, the same types of data fields that third-party developers could obtain through

their applications. JA 4181, 5056-58. Although Facebook's policies purportedly prohibited applications from selling data to advertisers, Facebook knew that many of its applications bought advertising themselves or shared their data with advertisers. An internal Facebook communication from March 2013 discussed one application that had been [redacted] JA 4521. Despite knowing that this application was violating its policies [redacted] Facebook never [redacted] JA 4521.

In 2014, two years after Facebook employees had identified a [redacted], Facebook began to close the spigot of friend data. It launched Graph API version 2.0, which generally did not allow applications to access friend data unless the friend had also installed the application. JA 726-27. However, existing applications were given until 2015 to transition to the new version, giving them access to friend data for an extra year. JA 739. Facebook granted many applications extensions on this one-year deadline, and it additionally offered several applications "private" APIs, which gave them access to a broader swath of data permanently. JA 4423, 4431-34. Even applications that fully transitioned to Graph API version 2.0 were not required to destroy the friend data they had already collected; that data was [redacted] JA 5125-27.

Facebook's efforts to restrict access to friend data came too late to prevent the

Cambridge Analytica data leak. In November 2013, Aleksandr Kogan launched an application using Graph API version 1.0, later named "*thisisyourdigitallife*." JA 808. The application was ostensibly a personality test, but really it was a mechanism to collect and monetize a massive amount of Facebook user data. Kogan informed Facebook that he was collecting [redacted]. JA 5148; *see* JA 5133-34, 5143-44, 5152-64. But he made clear in the application's privacy policy that he intended to [redacted] the user data that he collected, a blatant violation of Facebook's rules. JA 5023-24. Because Facebook did not vet applications at the time, no one at the company noticed. JA 4177.

Approximately [redacted] Facebook users installed Kogan's application, including [redacted] in the District. JA 824. But because Graph API version 1.0 allowed developers to siphon data about users' friends, Kogan was able to collect data on 87 *million* people. JA 824. That included an estimated [redacted] people in the District who never downloaded his application—more than half of the District's entire population. JA 825. The data collected included each user's [redacted]. JA 812-13.

True to his word, Kogan sold this data to Cambridge Analytica, which used it to create political advertising that generated millions of dollars in revenue for Facebook. JA 534-37, 2814-16, 4696-4704. Campaigns could target particular

users based on details about their daily lives that the users had never agreed to share with Cambridge Analytica—indeed, that they thought they were sharing with "Friends Only." *See* JA 4711-12. [redacted] JA 4533-43. Staff described the company as [redacted] that they suspected of [redacted] user data for advertising purposes. JA 4533. However, the [redacted] because Facebook lacked [redacted]. JA 5059-60.

On December 11, 2015, the Guardian published an article revealing that Kogan may have passed data obtained through his application to Cambridge Analytica. JA 813-14. Facebook [redacted]. JA 3184-86. [redacted] that this was a [redacted] violation of Facebook's policies against selling user data. JA 3184. Facebook requested that Kogan and Cambridge Analytica delete the user data they had obtained, JA 3184, but [redacted]. JA 4179-80, 4995. [redacted]. *See* JA 821. [redacted]. JA 4181, 5056-58.

Facebook continued to [redacted]

[redacted]. Facebook employees recognized that merely [redacted] Cambridge Analytica to delete its data was [redacted] JA 5016. In November 2016, Facebook employees noted that [redacted] and that [redacted] JA 4712. However, Facebook [redacted].

On March 17, 2018, journalists reported that Cambridge Analytica had received individual user data from Facebook (something the Guardian's previous reporting had not revealed), had not deleted the data after the 2015 reporting, and had used the data for advertising during the 2016 presidential election. *See* Matthew Rosenberg et al., *How Trump Consultants Exploited the Facebook Data of Millions*, N.Y. Times (Mar. 17, 2018), https://tinyurl.com/3es7dhh5. The public's reaction to this revelation was swift. [redacted] JA 5065-67, 5169-72. Facebook's stock value dropped by approximately 21% within nine days. JA 5174. Governmental bodies around the globe—including the U.S. Congress, the Federal Trade Commission ("FTC"), and a bipartisan coalition of 37 state attorneys general—launched investigations into Facebook's conduct. JA 822-23. Only after this public furor did Facebook notify users whose data had been

obtained by Cambridge Analytica. JA 825-27.

Facebook CEO Mark Zuckerberg testified that the Cambridge Analytica incident was "incredibly important," "relevant to a lot of people," and that people were "rightfully paying attention" to it. Senate at 131; JA 3858-60. He also recognized that users "certainly did not expect" their data to be sold and that the revelations had caused users significant "concern[]." Senate at 95, 135. He emphasized that users' expectation of "complete control" is "the most important principle for Facebook," because users assume that their information is going to "who they say it is going to" and no one else. Senate at 22.

2. Procedural History.

A. The District sues Facebook for violating the CPPA.

On December 19, 2018, the District sued Facebook for violating the CPPA. JA 78-98. The District alleged that Facebook made misleading statements to consumers about what data was accessible to third-party applications as well as its own enforcement capabilities. JA 88-95. It also alleged that Facebook failed to timely disclose the Cambridge Analytica data leak. JA 89. These failures violated the CPPA's prohibition on unfair and deceptive trade practices because they misrepresented and omitted material facts and used "innuendo or ambiguity" that had "a tendency to mislead." *See* D.C. Code § 28-3904(e), (f), (f-1).

Facebook moved to dismiss the District's complaint for lack of personal

jurisdiction and failure to state a claim, and alternatively moved to stay proceedings pending the outcome of ongoing multi-district litigation and an investigation by the FTC. JA 4. The Superior Court found that Facebook was subject to specific personal jurisdiction in the District based on its business transactions, JA 112-22, and that a stay was unwarranted, JA 128-30. The court further ruled that the District's complaint plausibly alleged violations of the CPPA based on Facebook's statements and omissions, concluding that "a reasonable consumer" could "find Facebook's disclosures ambiguous and misleading." JA 122-27.

B. The Superior Court strikes the District's expert.

On May 17, 2022, Facebook moved to exclude the testimony of the District's expert, Dr. Florian Schaub. JA 142-84. Dr. Schaub is an Associate Professor of Information and of Electrical Engineering and Computer Science at the University of Michigan. JA 2076. He has authored or co-authored more than 70 peer-reviewed articles and conference papers on issues of human-computer interaction, cybersecurity, and privacy. JA 1484. Dr. Schaub analyzed Facebook's policies, disclosures, and privacy controls to determine whether they were likely to mislead ordinary consumers regarding third-party access to user data. JA 1476-77. He concluded that Facebook's disclosures were confusing and difficult to read, and that relevant information was often outside the sections where a reasonable consumer would expect to find it. JA 1538-59. He also concluded that Facebook could have

made accurate disclosures, which would have affected user behavior. JA 1560-76.

Facebook argued that Dr. Schaub's testimony was merely his subjective opinion and insufficiently reliable to be presented to the jury because it was based on existing studies of user behavior rather than new surveys specific to Facebook. JA 156-62. It also criticized his readability testing for analyzing Facebook's disclosures as a whole rather than selected portions. JA 162-63.

The court held a hearing on Facebook's motion on November 7, 2022. JA 899-960. After hearing the parties' arguments, the court expressed doubt that the District really "need[ed]" expert testimony. JA 928. It also asked why "nobody double check[ed]" Dr. Schaub's analyses, since it viewed expert testimony as admissible only if it has been "audited" or "peer reviewed." JA 932-33. The court expressed confusion over Facebook's challenge to Dr. Schaub's readability study because it did not see anything "wrong" with analyzing "the whole document." JA 949. At the end of the hearing, the Court stated, "I don't know how I'm going to come out on this," and reserved decision. JA 956-57. One week later, the court granted Facebook's motion in a two-sentence order. The entirety of the court's analysis stated that the motion was granted "for the reasons stated in the opposition and in open Court on November 7, 2022." JA 961.

C. The Superior Court enters summary judgment for Facebook.

On June 1, 2023, the Superior Court granted Facebook's motion for summary

judgment. JA 1029-46. It began by rejecting the District's argument that claims for unintentional misrepresentation under the CPPA must be proved by a preponderance of the evidence and instead applied the clear-and-convincing standard applicable to claims of intentional fraud. JA 1034. The court then held that, as a matter of law, Facebook's statements and privacy settings could not have misled an ordinary consumer because the Data Use Policy notified users that their friends might "re-share" their information with third parties. JA 1036-39, 1041-42. It further held that Facebook's representations about its enforcement efforts could not have been misleading because they stated merely that Facebook "may" enforce its policies against applications, not that it "would" conduct such enforcement. JA 1039-41. The court also held that Facebook had no duty to inform its customers that their data had been sold to Cambridge Analytica. JA 1040-45. In granting Facebook's motion, the Superior Court exclusively cited Facebook's statement of material facts, JA 1030-45, and did not acknowledge any of the evidence that the District had presented in its opposition.[2] On June 29, 2023, the District timely appealed. JA 1047-52.

STANDARD OF REVIEW

This Court reviews a grant of summary judgment de novo. *Tolu v. Ayodeji*, 945 A.2d 596, 601 (D.C. 2008). The Court "conduct[s] an independent review of

---

[2] At the summary judgment hearing on March 21, the court acknowledged not having reviewed any of the parties' sealed filings, which included the vast majority of the District's exhibits and its responses to Facebook's factual summary. JA 1020.

the record, construing it in the light most favorable to the non-moving party," *Saucier v. Countrywide Home Loans*, 64 A.3d 428, 437 (D.C. 2013), and affording the non-movant "all favorable inferences which may reasonably be drawn from the evidentiary materials," *Tolu*, 945 A.2d at 601 (quoting *Beard v. Goodyear Tire & Rubber Co.*, 587 A.2d 195, 198 (D.C. 1991)). The movant is entitled to summary judgment only if it shows that there is no genuine issue as to any material fact and that "no reasonable juror could find for [the non-moving] party as a matter of law." *Biratu v. BT Vermont Ave., LLC*, 962 A.2d 261, 263 (D.C. 2008). The Court reviews the decision to admit or exclude expert testimony for an abuse of discretion. *Motorola Inc. v. Murray*, 147 A.3d 751, 755 (D.C. 2016) (en banc).

SUMMARY OF ARGUMENT

1. The Court should reverse the Superior Court's grant of summary judgment for Facebook because it is genuinely disputed whether Facebook's statements and omissions would be misleading to a reasonable consumer. Viewing the facts in the District's favor, a jury could conclude that Facebook violated the CPPA in three ways. *First*, Facebook did not adequately disclose the practice of friend sharing, and its settings gave consumers the misimpression that restricting access to "Friends Only" would truly limit information to only their friends. *Second*, Facebook's statements about third-party applications gave reasonable consumers the impression that Facebook had robust enforcement capabilities to protect user data,

when in truth it had virtually none. *Third*, Facebook's failure to notify affected users about the Cambridge Analytica data leak for two years was a material omission.

The Superior Court's decision misapplied several relevant legal principles. It misapplied the summary judgment standard because it accepted as true Facebook's description of the facts, even though many key facts are disputed. It also misinterpreted the CPPA because it assumed that truthful disclosures can never be misleading and that an omission is actionable only if there is an independent duty to disclose, both propositions that this Court has rejected. Finally, it applied the higher burden of proof applicable to claims for fraud, even though this is a case about unintentional misrepresentations.

2. The Superior Court also abused its discretion in excluding the District's privacy expert, Dr. Florian Schaub. The Superior Court's two-sentence order provided no reasoning, purporting to rest on its oral findings (even though it made none) and on the District's opposition to the motion to exclude, which makes no sense. Even assuming this was scrivener's error, there were no grounds to exclude Dr. Schaub's testimony. Dr. Schaub was qualified to testify, relied on appropriate data, and formed his opinions using reliable principles and methods. All of Facebook's objections to his testimony went to weight, not admissibility.

ARGUMENT

I. Summary Judgment Was Improper Because It Is Genuinely Disputed Whether Facebook's Statements Were Misleading To A Reasonable Consumer.

The CPPA is "an ambitious piece of legislation" meant to protect District residents from any unscrupulous business, even one as large and powerful as Facebook. *Howard v. Riggs Nat'l Bank*, 432 A.2d 701, 708 (D.C. 1981). The statute's "essential purpose" is to "assure that a just mechanism exists to remedy *all* improper trade practices" in the District. *Grayson v. AT&T Corp.*, 15 A.3d 219, 239 (D.C. 2011) (en banc) (quoting D.C. Code § 28-3901(b)(1)) (emphasis added). The Council defined the CPPA's terms "comprehensively" to effectuate the law's "broad remedial purposes." *DeBerry v. First Gov't Mortg. & Invs. Corp.*, 743 A.2d 699, 700 (D.C. 1999). The Council has also explicitly directed that the statute "be construed and applied liberally to promote its purpose." D.C. Code § 28-3901(c).

At its core, the CPPA "establishes an enforceable right to truthful information from merchants about consumer goods and services." *Id.* It does so by making it unlawful for "any person to engage in an unfair or deceptive trade practice." *Id.* § 28-3904. It goes on to enumerate a "long" but non-exhaustive list of prohibited practices, which are broadly defined and occasionally overlap. *Howard*, 432 A.2d at 708. They include "misrepresent[ing] as to a material fact which has a tendency to mislead," D.C. Code § 28-3904(e), "fail[ing] to state a material fact if such failure

tends to mislead," *id.* § 28-3904(f), and "us[ing] innuendo or ambiguity as to a material fact, which has a tendency to mislead," *id.* § 28-3904(f-1). Through its comprehensive language, the CPPA is intended "to provide procedures and remedies for a broad spectrum of practices which injure consumers." *Atwater v. D.C. Dep't of Consumer & Regul. Affs.*, 566 A.2d 462, 465 (D.C. 1989).

Importantly, the CPPA was specifically intended to make it easier to prove unfair trade practice claims "by eliminating the requirement of proving certain elements such as intent to deceive and scienter" that are required for common law fraud. *Fort Lincoln Civic Ass'n, Inc. v. Fort Lincoln New Town Corp.*, 944 A.2d 1055, 1073 n.20 (D.C. 2008). An unfair trade practice need not be intentional. *Frankeny v. Dist. Hosp. Partners, LP*, 225 A.3d 999, 1004-05 (D.C. 2020); *Grayson*, 15 A.3d at 251. Nor does it matter whether "any consumer is in fact misled, deceived, or damaged." D.C. Code § 28-3904. Rather, the main question in a CPPA case is "how the practice would be viewed and understood by a reasonable consumer," *Pearson v. Chung*, 961 A.2d 1067, 1075 (D.C. 2008), which is "a question of fact for the jury and not a question of law for the court," *Saucier*, 64 A.3d at 445 (quoting *Green v. H&R Block, Inc.*, 735 A.2d 1039, 1059 (Md. 1999)).

A. Viewing the facts in the District's favor, a reasonable person could find that Facebook engaged in unfair or deceptive practices.

Examining the evidence in the light most favorable to the District, a jury could find that Facebook's statements, omissions, and innuendo violated the CPPA, any

one of which would be enough to merit a trial. Whether Facebook's representations and omissions were material and had "a tendency to mislead" an ordinary consumer were hotly disputed questions of fact that should have been left to a jury.

1. Consumers could have been misled about friend sharing.

An ordinary Facebook user could reasonably have been misled about what personal information was accessible to third-party applications through their friends. In particular, a reasonable consumer could have come away with the misimpression that the profile information they shared with "Friends Only" would be shared *only* with friends, not automatically forwarded to unknown third-party applications.

An ordinary consumer's understanding of what information would be shared must be assessed based on the evidence as a whole,[3] beginning with Facebook's broad public statements emphasizing the importance of "privacy" and "control." Facebook's SRR stressed that "privacy is very important," and that users "can control how [their information] is shared through [their] privacy and application

---

[3] *See Wetzel v. Cap. City Real Est., LLC*, 73 A.3d 1000, 1004-05 (D.C. 2013) (assessing whether dozens of representations taken together tended to mislead); *see also POM Wonderful, LLC v. FTC*, 777 F.3d 478, 490 (D.C. Cir. 2015) (explaining that whether an advertisement is "unfair" or "deceptive" under the Federal Trade Commission Act, 15 U.S.C. § 45(a)(1), is based on a reasonable consumer's "overall net impression," and "whether at least a significant minority of reasonable consumers would likely interpret the ad to assert the claim" (cleaned up)); *Bell v. Publix Super Mkts., Inc.*, 982 F.3d 468, 476 (7th Cir. 2020) (in assessing whether labeling is misleading to a reasonable consumer, "the context of the entire packaging is relevant").

settings." JA 2187. Facebook asserted that an application must have a user's "permission" to access the user's content and information, without mentioning that any application could also access information through the user's friends. JA 2187.[4]

In light of the emphasis on privacy and control, a reasonable user would look to Facebook's "Privacy Settings" to understand what information was being shared and with whom. But as explained, *supra* pp. 6-11, those settings were misleading. They gave users the illusion of control by allowing them to restrict access to certain parts of their profile from "Everyone" to "Friends of Friends," and "Friends Only." JA 1526. Yet even if a user restricted *every* field to "Friends Only," all of that information would still be available to third-party applications through friend sharing. JA 1525-30. In fact, the privacy settings did not address applications at all.

To actually restrict access to third-party applications, a user would need to seek out "Application Settings," a page that would display only applications they used, not those used by their friends. JA 1528. Then, they would need to click another layer down into "info accessible through your friends." JA 1528-30. Even this page did not make clear that sharing applied to applications that the user themselves did not use. Instead, it emphasized that sharing was needed to make the

---

[4] Despite publicly telling users that they "own" and "control" all of their information, JA 2187, Facebook has justified the practice of friend sharing by claiming that a user's *friends* actually "control[]" any information that anyone has shared with them. JA 398.

applications "more social"—implying that only mutually used applications would access this information. JA 1530. The only way to prevent this access completely (and for certain categories of information like name and gender) would be to turn off Platform entirely, eliminating the user's ability to use any applications.

Other settings similarly obfuscated friend sharing. If a user entered the Help Center, they would find various pages about "App Visibility and Privacy," but these would tell the user only about the applications *they* used, not those their friends used. JA 457. "Privacy Checkup," "Privacy Basics," "Privacy Tour," and "Privacy Shortcuts" all focused on posts, not profile information, and on applications the user had downloaded, not those used by friends. JA 2508-12. The critical disclosure about friend sharing was buried in a subpage titled "Controlling what is shared when the people you share with use applications," which was not visible from the "App Visibility and Privacy" page. JA 457-60. This information was later moved to a page called "About Facebook Platform," which does not indicate from its title that it has anything to do with third-party applications or friend sharing. JA 461.

Even where Facebook claims it disclosed friend sharing, it failed to give users clear guidance about what information was transmitted. The Data Use Policy compared friend sharing to email, implying that the information could only be transmitted if a friend actively "re-shared" it. JA 2220. That analogy was misleading. It is one thing to understand that a friend could choose to re-forward an

email to others; it is another to understand that every email to every friend is automatically being forwarded to an unknown list of third parties.

Even Facebook acknowledged that users did not understand its disclosures and settings. In a 2014 presentation, Facebook stated that users receive [redacted] about friend sharing and that information is transferred to third-party applications [redacted] JA 4095. This conclusion was supported by the company's studies, which showed that users [redacted]. JA 4020-29, 4044-71. Zuckerberg acknowledged after the Cambridge Analytica incident that "long privacy policies are very confusing," and that the company "do[es] not expect that most people will" read them. Senate at 15; *see also* JA 4107 (Facebook COO Sheryl Sandberg acknowledging that Facebook's privacy controls were "hard to understand and hard to find"). In short, a reasonable consumer—even one diligent enough to review Facebook's privacy statements and settings—could come away without realizing that third-party applications they never used would automatically receive all of their personal information through friend sharing.

Facebook's vague, confusing, and sometimes contradictory statements are precisely what the CPPA was designed to address by prohibiting misrepresentations, omissions, and ambiguities that tend to mislead consumers. D.C. Code § 28-3904(e), (f), (f-1). This Court has long made clear that context and placement are

key in applying the reasonable consumer standard. In *Center for Inquiry*, this Court concluded that an ordinary consumer could be confused about the comparative efficacy of homeopathic drug products based on their placement on store shelves alongside FDA-approved over-the-counter drugs, despite the differences in product labeling. *Ctr. for Inquiry Inc. v. Walmart, Inc.*, 283 A.3d 109, 120-21 (D.C. 2022). The Court explained that "the reasonable consumer standard does not presume, *at least as a matter of law*, that reasonable consumers will test prominent front-label claims by examining the fine print on the back label." *Id.* at 121 (quoting *Bell*, 982 F.3d at 477). Similarly, an ordinary consumer cannot be expected to look behind Facebook's prominent statements implying that users could "control" access to their information by changing their privacy settings. *See Fanning v. FTC*, 821 F.3d 164, 171-72 (1st Cir. 2016) (examining statements across multiple pages of a website—not just its legal disclaimers—to assess what a reasonable consumer would believe).

2. Consumers could have been misled about Facebook's enforcement capabilities.

A reasonable consumer also could have been misled by Facebook's statements suggesting it had powerful tools to protect user data when it did not. In various places, Facebook indicated that it would enforce its data policies against applications and other third parties. It said that it would "require applications to respect [user] privacy." JA 2187. It said that applications would be "allowed" to use information only in connection with the user who downloaded it, JA 2220, and

could collect only the data needed to operate the application, JA 2189. It said that it would prohibit applications from selling user data or transferring it to advertisers. JA 2189-90. It said that applications would be required to have privacy policies that disclosed how data would be used, and that data could not be transferred outside of an application. JA 2189-90. Facebook asserted that it could "analyze [the] app, content, and data for any purpose," to "audit" it to "ensure [the] application is safe for users," and could require applications to delete data if it was used improperly. JA 2190. In reality, each of these statements was misleading.

By phrasing these things as enforcement measures Facebook "can" take, Facebook implied that it actually had the capability to conduct this enforcement. As one court examining the same disclosures has explained, a "plausible interpretation of the disclosure is that it assures users that Facebook is actively policing the activities of app developers on its platform." *In re Facebook, Inc., Consumer Priv. User Profile Litig.*, 402 F. Supp. 3d 767, 794 (N.D. Cal. 2019). It would also be reasonable for a reader to assume that "the word 'allowed' references a technological block of sorts" that would "physically prevent app developers from being able to 'see' friend information outside the context of their interactions with users." *Id.* Elsewhere in the same policy, for instance, Facebook uses the word "allowed" in this way, by stating, "If someone clicks on a link to another person's timeline, they'll only see the things that they are allowed to see." JA 2218.

The image of a robust enforcement system—perhaps with automated tools to physically prevent data from being misdirected—was an illusion. Facebook had no ability to audit applications or prevent consumers' data from being misused; in fact, it had [redacted] at all into what developers were doing with the data they collected. JA 4494-95. [redacted] JA 4496-97, 4910, 4919. That team would [redacted]. JA 4530, 4693, 4999. [redacted] JA 4755.

It is easy to see how these statements could mislead an ordinary consumer. If a private security company advertised that it "allowed" only legitimate contractors on a construction site and would "require" all visitors to show identification, that is what one would expect the company to do. If the company further stated that it "could" analyze each contractor's roster of employees and "audit" their background for security risks, it would be reasonable to assume the company had that capability. If it later turned out that the company had only one employee who could not possibly check the identification of every entrant, did not have the tools necessary to conduct background checks, and never followed up when visitors appeared to be trespassing,

then those representations would all be misleading.

3. Consumers could have been misled by Facebook's failure to notify users about the data leak for more than two years.

An ordinary consumer also could have been misled by a critical omission: Facebook's decision not to tell affected users that their information had been transferred to Cambridge Analytica. This omission is actionable on its own, but it also renders Facebook's assertions that it had powerful enforcement tools to protect user data from malicious applications even more misleading. The decision not to inform users that those tools had failed spectacularly could have deceived users into believing that their information was safer than it was. Although Facebook eventually informed affected users in 2018, that was several years too late.

Facebook was on notice that Kogan intended to sell user data when he launched his application in November 2013. Kogan personally told Facebook that he was using the application to [redacted]. JA 5023-24. Because Facebook's oversight of third-party applications was so weak, no one noticed these red flags. Then, [redacted]. JA 4533-43. The [redacted] went nowhere. JA 5059-60.

In December 2015, public reporting revealed that Cambridge Analytica may

have obtained Facebook user data improperly, but it did not reveal the full scope of the leak. [redacted] JA 3184-86. At this point, Facebook asked Kogan and Cambridge Analytica to delete the user information that they had obtained, [redacted]. JA 5016. Facebook did not conduct any type of audit to ensure that the information was deleted, a decision Facebook has since acknowledged was a "mistake." Senate at 16-17. It did not inform any affected users, including the hundreds of thousands in the District, another decision it has recognized was a "mistake." Senate at 321. [redacted], but Facebook did not ban Cambridge Analytica, yet another conceded "mistake." Senate at 91. Facebook did not inform any affected users until 2018—when further reporting made continued silence impossible.

In light of all this evidence, a jury could find that Facebook's decision not to inform affected users about Cambridge Analytica tended to mislead. Although there is no obligation under the CPPA that a consumer actually be misled, "evidence that some customers actually misunderstood the thrust of the message is significant support for the finding of a tendency to mislead." *Beneficial Corp. v. FTC*, 542 F.2d 611, 617 (3d Cir. 1976). Here, the public reaction to Facebook's belated disclosure in 2018 strongly suggests that consumers did not understand the scope of the

problem when it was first reported in 2015. Zuckerberg himself explained that consumer reaction was so strong in 2018 because "people certainly did not expect this developer to sell the data to Cambridge Analytica." Senate at 95. That mismatch in expectations is strong evidence of a tendency to mislead.

4. Consumers could have found these misrepresentations and omissions material.

A reasonable jury could find that Facebook's misrepresentations and omissions were material. A representation is material if a reasonable person would consider it important in determining his or her choice of action, or if the speaker "knows or has reason to know" that the recipient is likely to regard it as such. *Saucier*, 64 A.3d at 442. Critically, materiality is measured from the perspective of a reasonable but "unsophisticated" consumer. *Id.* "Ordinarily the question of materiality should not be treated as a matter of law," but should instead be left to the jury to decide as a question of fact. *Id.* (quoting *Green*, 735 A.2d at 1059). This case is no exception. Given Facebook's relentless focus on giving users the impression of "control" over their information, a jury could find as a matter of fact that Facebook's misrepresentations and omissions were material.

Reasonable consumers could consider friend sharing, Facebook's enforcement capabilities, and the Cambridge Analytica data leak to be material in deciding how to interact with Facebook. Users who understood that their information could be transferred through friends to any number of unknown third-

party developers may have weighed this information when deciding what applications to use, who to add as friends, and whether to use Facebook at all. Users who understood that Facebook lacked the technological capability or resources to effectively audit applications—and that some applications had already violated Facebook's terms by transferring user data—may have reassessed whether to turn off Platform completely to block all applications. Ample evidence in the record would permit the jury to draw these conclusions:

First, Facebook has long acknowledged that the perception of privacy and control is central to its business and critical to the success of Platform specifically. *E.g.*, JA 3447, 3693, 3715. Facebook's self-declared "mission" is "to enable people to share what they want with exactly who they want." JA 3063. Zuckerberg himself has testified that "it is important to tell people exactly how the information that they share on Facebook is going to be used" and that "giving people complete control" is "the most important principle for Facebook." Senate at 15, 22. If users realized that their information was actually being shared more broadly than they intended, the company "know[s]" users would not "feel comfortable using [Facebook's] services." Senate at 135. Facebook's own studies of user behavior show that users [redacted]. JA 3986-4075.

Second, Zuckerberg testified that the Cambridge Analytica incident was a shock to most users. But it would not have been if users had been fully informed

about friend sharing and Facebook's minimal oversight of third-party applications. It certainly would not have come as a surprise in 2018—after the presidential election—if Facebook had told affected users about it back in 2015 or 2016. Zuckerberg testified that he "would hope" that Facebook's data practices are "not surprising to people" but acknowledged that the Cambridge Analytica incident had surprised many, because "people certainly did not expect" that their data could be taken by developers for resale. Senate at 95. He also acknowledged that it was "clearly" a "mistake" not to inform users about the Cambridge Analytica incident back when Facebook first learned about it in 2015. Senate at 126, 321. That was because Facebook convinced users that their data was safe, when in fact Facebook knew that millions had already had their data sold in violation of its policies.

Third, that users considered the misrepresentations and omissions material is evident from the overwhelming and negative public response to revelations about Cambridge Analytica. After the incident was revealed, [redacted], and Facebook's stock lost more than 20% of its value. JA 5065-67, 5169-74. Facebook may argue that there is no causal link between these events, but a jury certainly could reasonably infer that some users did change their behavior once the full facts were known, which would support a finding of materiality.

B. In entering summary judgment for Facebook, the Superior Court committed three principal legal errors.

1. The court ignored genuine disputes of material fact.

In granting summary judgment to Facebook, the Superior Court relied exclusively on Facebook's version of the facts, contrary to the well-established summary judgment standard. *E.g.*, *Saucier*, 64 A.3d at 437. Specifically, the court cited 86 paragraphs from Facebook's statement of material facts, even though 32 of those paragraphs had been fully or partially disputed by the District. *See* JA 631-867. The court did not acknowledge any of those disputes, nor did it acknowledge any of the 5,000 pages of evidence that the District had submitted in support of its claim. This error alone merits reversal.

Many of the facts the Superior Court assumed to be true were genuinely disputed by other evidence in the record. For instance, the court stated that Facebook's privacy tools were "easy to locate" and that a reasonable user could "readily follow along" in changing their privacy settings. JA 1042. But there is overwhelming evidence that this was not true. The District presented Facebook's own internal studies showing that users [redacted]. *See* JA 3986-4040. One study showed that a focus group [redacted] the very settings that the court characterized as "easy" to locate. JA 4054. Other studies showed that users [redacted] JA 4033. Even Facebook's COO acknowledged that privacy settings were [redacted]

[redacted] JA 4107.

The court also accepted Facebook's assertion that it "used a range of measures to monitor third-party apps and ensure compliance, including both manual review and automated review." JA 1031. The evidence actually showed that Facebook conducted no pre-review of applications prior to 2014 and that [redacted] JA 4172, 4493, 4496-97, 4910, 4919. Internal documents also showed that Facebook's enforcement was [redacted]. JA 4462-66. And one key piece of evidence that Facebook's systems were inadequate was that Kogan was able to obtain data on 87 million Americans while brazenly declaring his intention to sell the information.

In addition, the court adopted Facebook's timeline of events regarding the Cambridge Analytica leak despite contrary evidence. For example, the court accepted Facebook's claim that it first "became aware" of Kogan's actions based on press coverage in December 2015. JA 1031-32. The District presented competing evidence showing that Facebook [redacted], and that [redacted]. JA 4533-43, 5133-34, 5152-64. The court also accepted Facebook's contention that Facebook "learned from media inquiries that Cambridge Analytica may not have destroyed the data and may have used it for political advertising, contrary to its prior

representations." JA 1032. That too was contradicted by the District's evidence, which showed that employees at Facebook [redacted]. JA 4712.

In other instances, the court viewed evidence in the light most favorable to Facebook, rather than the other way around. For example, the court stated that Facebook adequately disclosed that it was "not responsible" for the acts of third parties, JA 1040, and "never guaranteed how it would proceed in an enforcement investigation" because it only said that it "*may* enforce" its policies. JA 1040. But the District identified many *other* disclosures that give a different impression. Facebook said that applications would be "allowed" to use data only in connection with the user who gave the permission, and it said that Facebook would "require" applications to respect user privacy. JA 2187, 2220. And although Facebook did characterize its enforcement powers as things it "can" do, a reasonable reader could understand this to mean Facebook had the capability to conduct this oversight, even if it maintained some level of discretion on how to use that power. In reality, Facebook could not do many of the things it told users it could—like audit applications—because it lacked the necessary resources and technological capabilities.

In another example, the court said that Facebook adequately disclosed friend sharing in the Data Use Policy because the policy said that friends could "re-share"

information. JA 1036. But a reasonable consumer could read this statement as implying that a friend would need to *actively* reshare information for it to be made public, much like the email example Facebook highlighted in the same paragraph. Instead of construing this ambiguous disclosure in the light most favorable to the District, as the law requires, the court simply accepted Facebook's interpretation.[5]

2. The court misapplied the CPPA.

The Superior Court also assumed that truthful disclosures—no matter their context or omissions—cannot be misleading under the CPPA. JA 1035, 1037-38, 1041. That is incorrect. A "representation may be misleading . . . even if true," such as when a speaker omits material information or context. *Ctr. for Inquiry Inc.*, 283 A.3d at 120 n.11; *see* D.C. Code § 28-3904(e), (f), (f-1). In *Frankeny*, for example, this Court reversed a grant of summary judgment in favor of a hospital on a CPPA claim where the plaintiff contended that the hospital's disclosures, although technically accurate, did not give her reasonable notice that her surgery would be performed by a medical resident rather than her doctor of choice. 225 A.3d at 1008-09; *see also Ctr. for Inquiry*, 283 A.3d at 121 (reversing dismissal of CPPA claims

---

[5] The court also cited (at JA 1036-37) two other passages from the Data Use Policy, but these imply that friend sharing was limited to mutually used applications. The first stated that friend sharing made an application "more personalized and social" by letting it know "which of [a user's] friends is also using it." JA 2220. The second states that making information "public" means it will be accessible to "applications . . . you and your friends use," which again suggests mutuality and also does not address information the user has made non-public. JA 2214.

premised on factually accurate but allegedly misleading labeling and placement of homeopathic products). The Superior Court's contrary rule would insulate any misleading statement that is literally accurate, even if it "deceived most consumers, and even if it had been carefully designed to deceive them," which is not the law. *Bell*, 982 F.3d at 476.

The Superior Court also held that Facebook had no legal "duty" to provide users with additional information about friend sharing or disclose the Cambridge Analytica data leak when it first learned of it. JA 1041-43. But the CPPA does not require an independent "duty to disclose information." *Saucier*, 64 A.3d at 444. Again looking to *Frankeny* as an example, nothing in the Court's analysis suggested that the plaintiff was required to prove that the hospital had an independent duty to disclose who would perform her surgery in order to prevail. 225 A.3d at 1008-09.

In support of its ruling, the Superior Court relied on three decisions from other jurisdictions applying different legal standards. JA 1033 n.2. *First*, it cited a passage from an order in a shareholder securities case stemming from the Cambridge Analytica leak. *In re Facebook, Inc. Sec. Litig.*, 405 F. Supp. 3d 809, 846 (N.D. Cal. 2019). That paragraph is of little relevance here because it was analyzing whether Facebook's statement *from 2018* that users had given their "consent" met the Private Securities Litigation Reform Act's "exacting requirements for pleading falsity." 405 F. Supp. 3d at 837 (cleaned up). It was not analyzing whether Facebook's privacy

policies or settings would be misleading to a reasonable consumer. In any event, the Ninth Circuit ultimately reversed much of the district court's decision, finding that the shareholders *had* adequately alleged that Facebook "falsely represented to users that they had control over their data on the platform." *In re Facebook, Inc. Sec. Litig.*, 87 F.4th 934, 957 (9th Cir. 2023). *Second*, the Superior Court cited an unpublished decision applying the standard for *intentional* consumer fraud under Illinois law. *See People v. Facebook, Inc.*, No. 2018-CH-03868, at 10-11 (Ill. Cir. Ct. Mar. 8, 2021).[6] That decision assessed only whether Facebook intended to deceive consumers into thinking their data was "guaranteed to be safe," which has never been the District's theory. *Third*, the Superior Court cited *Smith v. Facebook, Inc.*, 745 F. App'x 8 (9th Cir. 2018), which is similarly inapposite because it concerned Facebook's collection of browsing data, not the distribution of information to third-party applications.

3. The court applied the wrong burden of proof.

The Superior Court held the District to a "clear and convincing" burden of proof. JA 1034 & n.3. That was incorrect; claims of unintentional misrepresentation under the CPPA must be proved by a preponderance of the evidence. The preponderance standard is "the default rule for civil cases," *CIGNA Corp. v. Amara*,

---

[6] It is not clear whether the trial court even had the full text of this decision because it is not available in any online database and Facebook did not supply a copy as an exhibit. The decision is attached as an addendum for reference.

563 U.S. 421, 444 (2011), and exceptions are "rare," *Raphael v. Okyiri*, 740 A.2d 935, 957 (D.C. 1999). "Where no standard is specified in the statute and due process does not compel a different result, it ordinarily applies." *Bailey v. United States*, 251 A.3d 724, 729 (D.C. 2021). Nothing in the text of the CPPA indicates that the Council intended to depart from the ordinary standard of proof.

In applying the clear-and-convincing standard, the Superior Court cited *Pearson v. Chung*, 961 A.2d 1067 (D.C. 2008). JA 1034 n.3. *Pearson* states that "the clear and convincing evidence standard applies to claims of *intentional* misrepresentation under the CPPA." *Id.* at 1074 (emphasis added) (quoting *Caulfield v. Stark*, 893 A.2d 970, 976 (D.C. 2006)). That is because claims of intentional misrepresentation sound in fraud and can seek punitive damages, which at common law required proof by clear and convincing evidence. *See Osbourne v. Cap. City Mortg. Corp.*, 727 A.2d 322, 325-26 (D.C. 1999). Because *Pearson* only dealt with a claim of intentional misrepresentation, the Court had no occasion to address what burden of proof would apply to unintentional claims.

But this Court has settled the once "open question," *Caulfield*, 893 A.2d at 977, and clarified that the CPPA *does* encompass actions for unintentional misrepresentations like those the District has brought here. *Fort Lincoln*, 944 A.2d at 1073. *Fort Lincoln* made clear that the CPPA "intended to overcome the pleadings problem associated with common law fraud claims by eliminating the requirement

of proving certain elements such as intent to deceive and scienter." *Id.* at 1073 n.20. The Court also strongly implied that the CPPA did away with other requirements of fraud claims like the clear-and-convincing standard. The Court said that once a plaintiff "prove[s] a failure to disclose material information," "liability attaches" and the court must turn to damages. *Id.* at 1073. It said nothing about that proof needing to be by clear and convincing evidence. *See id.* at 1073 n.21 (recognizing that *Osborne* applied the clear-and-convincing standard to claims of intentional misrepresentation under the CPPA but had left open the question of "whether the CPPA also embraces claims of unintentional misrepresentation" (quoting *Caulfield*, 893 A.2d at 976)).

To be sure, in *Frankeny*, the Court repeated the clear-and-convincing standard from *Pearson* even though it was addressing a claim for unintentional misrepresentation. 225 A.3d at 1005. But this single-sentence recitation was dictum. Neither party briefed the issue; they assumed without analysis that the higher standard applied. *See* Br. for Appellant at 15 (No. 18-CV-628), 2018 WL 11196904; Br. for Appellees at 10 (No. 18-CV-628), 2018 WL 11196906. It was also unnecessary to the Court's holding that the plaintiff's evidence was sufficient to overcome a motion for summary judgment—by definition, this would also have been true under the lower preponderance standard. *Frankeny*, 225 A.3d at 1008-10. Accordingly, the question was "neither brought to the attention of the court nor ruled

upon," and cannot "be considered as having been so decided as to constitute precedent[]." *United States v. Debruhl*, 38 A.3d 293, 298 (D.C. 2012) (quoting *Murphy v. McCloud*, 650 A.2d 202, 205 (D.C. 1994)).[7]

II. Excluding The District's Expert Was An Abuse Of Discretion.

The Superior Court abused its discretion in excluding the District's expert, Dr. Schaub, who was well qualified to opine on whether an ordinary user would be able to locate and understand Facebook's privacy policies and settings. Although Dr. Schaub's testimony was not necessary for the District to prove its claims, it was admissible evidence that the District should be permitted to present at trial.

A. The Superior Court's order contains no reasoning.

The Superior Court's order excluding Dr. Schaub's testimony was an abuse of discretion first because the court did not provide any logical explanation for its action. In exercising its discretion to admit or exclude expert testimony, the Superior Court had "an obligation to make a record that elucidates the factors that contributed to the . . . decision and upon which it was based." *In re Gardner*, 268 A.3d 850, 859

---

[7] Even if the Court disagrees and finds the clear-and-convincing evidence standard applies, the District's evidence is sufficient to reach a jury. Clear and convincing evidence "lies somewhere between preponderance of the evidence and evidence probative beyond a reasonable doubt"; it is evidence that "would produce in the mind of the trier of fact a firm belief or conviction as to the facts sought to be established." *In re Est. of Nethken*, 978 A.2d 603, 607 (D.C. 2009) (quoting *In re Ingersoll Tr.*, 950 A.2d 672, 693 (D.C. 2008)). For all of the reasons discussed *supra* in Part I.A, a jury could form a "firm belief" that Facebook's actions were likely to mislead an ordinary consumer as to material facts.

(D.C. 2022) (cleaned up); *see Sanchez v. District of Columbia*, 102 A.3d 1157, 1161 (D.C. 2014) ("The proper exercise of discretion requires that a valid reason be given or be discernable from the record."). "Without such an explanation, [this] [C]ourt cannot assess whether the Superior Court reasonably exercised its discretion." *Gardner*, 268 A.3d at 859.

The order excluding Dr. Schaub contains no reasoning whatsoever. It states that the court was excluding the testimony "for the reasons stated in the opposition and in open Court on November 7, 2022." JA 961. But the District's *opposition* to the motion cannot provide an explanation for why the court granted it, and the court never "stated" any "reasons" at the hearing, it merely asked questions and then expressly reserved decision. JA 956. The Superior Court's ruling was thus a textbook abuse of discretion. *Featherson v. Educ. Diagnostic Inst., Inc.*, 933 A.2d 335, 338 (D.C. 2007).

B. Dr. Schaub's testimony is admissible under *Daubert*.

Even assuming the Superior Court's reference to the District's "opposition" was a scrivener's error, there were no valid grounds to exclude Dr. Schaub's testimony. This Court applies the federal standard for the admissibility of expert opinions. *Motorola*, 147 A.3d at 757 (adopting the test from Fed. R. Evid. 702 and *Daubert v. Merrell Dow Pharms., Inc.*, 509 U.S. 579 (1993)). Under that test, the trial court must be satisfied that "(1) the witness is qualified as an expert; (2) the

witness's expertise will help the trier of fact to understand the evidence or to determine a fact in issue; (3) the witness's testimony is based on sufficient facts or data; (4) the testimony is the product of reliable principles and methods; and (5) the expert has reliably applied the principles and methods to the facts of the case." *Lewis v. United States*, 263 A.3d 1049, 1059 (D.C. 2021) (cleaned up). "The trial court's role as gatekeeper is not intended to serve as a replacement for the adversary system." *Motorola*, 147 A.3d at 757 (cleaned up). "Shaky but admissible evidence is to be attacked by cross examination, contrary evidence, and attention to the burden of proof, not exclusion." *Primiano v. Cook*, 598 F.3d 558, 564 (9th Cir. 2010).

Dr. Schaub's testimony met all the requirements for admissibility. *First*, he is "qualified" to offer expert testimony, and Facebook has never argued otherwise. *Lewis*, 263 A.3d at 1059; *see* JA 156. He is a tenured professor at the University of Michigan and has authored more than 70 peer-reviewed works on human-computer interaction, cybersecurity, and privacy. JA 1484, 2076. His work is heavily cited, and he has served as a subject-matter expert for the FTC. JA 1484-90.

Second, Dr. Schaub's testimony will help the jury understand the evidence. The threshold for whether evidence is relevant "is not a stringent one." *Lewis*, 263 A.3d at 1064. Demonstrating consumer perceptions "[t]ypically" involves expert testimony. *In re McCormick & Co., Inc., Pepper Prod. Mktg. & Sales Pracs. Litig.*, 422 F. Supp. 3d 194, 248 (D.D.C. 2019); *see, e.g.*, *Clevenger v. Welch Foods Inc.*,

No. SACV 20-01859, 2022 WL 18228293, at *3-*5 (C.D. Cal. Dec. 28, 2022); *In re JUUL Labs, Inc., Mktg. Sales Pracs. & Prod. Liab. Litig.*, 609 F. Supp. 3d 942, 1007-10 (N.D. Cal. 2022); *Price v. L'Oreal USA, Inc.*, No. 17 Civ. 614, 2020 WL 4937464, at *3 (S.D.N.Y. Aug. 24, 2020). Although the trial court at times expressed skepticism that any expert testimony was "need[ed]" in this case, JA 928, that is not the standard for admissibility. *See Motorola*, 147 A.3d at 757 n.8. Because Dr. Schaub's testimony was "logically probative of some fact in issue," it was relevant. *Plummer v. United States*, 813 A.2d 182, 188 (D.C. 2002) (quoting *Dockery v. United States*, 746 A.2d 303, 306 (D.C. 2000)).

Third, Dr. Schaub's opinions were based on sufficient facts and data. Dr. Schaub conducted his analysis using all of Facebook's privacy policies from the relevant time period, as well as relevant user interfaces like privacy settings. JA 1497-98. These are the materials the District contends were misleading and that Facebook contends, as a matter of law, absolve it of liability. Facebook has never identified specific other materials that it believes Dr. Schaub should have reviewed, but to the extent there are any, that goes to the weight, not admissibility, of his testimony. *Govan v. Brown*, 228 A.3d 142, 155 (D.C. 2020). Nothing in the trial court's questions at the hearing suggested it viewed the underlying materials as insufficient to support Dr. Schaub's analysis.

Fourth, Dr. Schaub used reliable principles and methods to form his

testimony, primarily readability tests and content analysis. Dr. Schaub explained that the readability tests he employed are "widely used to set and test readability requirements for public and private sector documents." JA 1535. He also testified that he had used the same readability tests in his peer-reviewed research. JA 2062, 2077. Dr. Schaub's content analysis was likewise a reliable method for determining what a reasonable consumer would understand from Facebook's disclosures and settings. He cited dozens of peer-reviewed articles endorsing the technique as a method of evaluating privacy policies, data-breach disclosures, and website privacy controls—the exact types of materials he was evaluating here. JA 1531-32.

Facebook offered little argument that either readability analysis or content analysis was an unreliable method in the abstract. It criticized content analysis as subjective and over-reliant on Dr. Schaub's experience, but these are not grounds to exclude the testimony. It is well established that an expert may "draw a conclusion from a set of observations based on extensive and specialized experience." *Kumho Tire Co. v. Carmichael*, 526 U.S. 137, 156 (1999). In such cases, "the method is the application of experience to facts." *Price*, 2020 WL 4937464, at *3 (quoting *Scott v. Chipotle Mexican Grill, Inc.*, 315 F.R.D. 33, 50 (S.D.N.Y. 2016)). Dr. Schaub explained that he used the same methodology he regularly employs in his peer-reviewed research, which is more than sufficient to demonstrate its reliability.

Facebook also argued that Dr. Schaub should have tested his theories using

surveys, and the Superior Court likewise questioned whether his analysis should have been "audited" or "peer reviewed." JA 932-33. But "expert reports regarding consumer perception need not be based on scientific surveys"; experts "may testify based on their own experience." *Price*, 2020 WL 4937464, at *5; *see Lytle v. Nutramax Laboratories, Inc.*, No. ED CV 19-0835, 2022 WL 1600047, at *5 (C.D. Cal. May 6, 2022). An expert's decision not to "conduct a market survey on consumer perceptions . . . ultimately goes to the weight of the testimony, not admissibility." *Hobbs v. Brother Int'l Corp.*, No. CV151866, 2016 WL 7647674, at *4 (C.D. Cal. Aug. 31, 2016).

Fifth, Dr. Schaub reliably applied those principles to this case. He explained that he proceeded as he would in the field at each step of his analysis. *See* JA 1531-34. He explained that he employed a "mental models" approach, which is "central to behavioral research, cognitive reasoning and decision research, and human-computer interaction research," to determine how an ordinary consumer would understand Facebook's policies and disclosures. JA 1533-34. For each of his opinions, he provided citations to peer-reviewed research supporting his conclusions. JA 1534-76.

Facebook offered no persuasive argument on why Dr. Schaub's readability analysis was unreliable. Its only argument was that Dr. Schaub should have limited his analysis to specific passages of Facebook's policies, rather than examining the

policies as a whole. But as even the trial court recognized, this argument makes little sense because there is nothing wrong with analyzing the documents in their entirety. JA 949. The reasonable consumer standard requires examining all of the available evidence that a reasonable consumer might encounter. *See supra* note 3. It was in part *because* Facebook buried relevant disclosures in long, difficult to read documents that users had trouble finding or understanding those disclosures.

Facebook took issue with how Dr. Schaub conducted his content analysis, but its objections are unfounded. It argued that content analysis requires multiple reviewers to compile a codebook, which Dr. Schaub did not use here. But there are multiple methods of conducting content analysis, some of which do not require a codebook or multiple annotators. *See* JA 2095. As Dr. Schaub explained, there was no need to compile a codebook here because he was the only reviewer and was not conducting a comparative analysis across multiple companies. JA 1532. That testimony was supported by peer-reviewed articles (not authored by Dr. Schaub) summarizing different approaches to content analysis. JA 2079-2115. To the extent Facebook has any critiques of Dr. Schaub's method, it will be free to raise those in cross examination or through its own rebuttal expert.

CONCLUSION

For the foregoing reasons, the judgment below should be reversed.

Respectfully submitted,

BRIAN L. SCHWALB
Attorney General for the District of Columbia

CAROLINE S. VAN ZILE
Solicitor General

ASHWIN P. PHATAK
Principal Deputy Solicitor General

GRAHAM E. PHILLIPS
Deputy Solicitor General

/s/ Jeremy R. Girton
JEREMY R. GIRTON
Assistant Attorney General
Bar Number 888304147
Office of the Solicitor General

Office of the Attorney General
400 6th Street, NW, Suite 8100
Washington, D.C. 20001
(202) 724-2029
(202) 741-8786 (fax)
jeremy.girton@dc.gov

March 2024

Public Version

ADDENDUM

People v. Facebook, Inc., No. 2018-CH-03868 (Ill. Cir. Ct. Mar. 8, 2021)

IN THE CIRCUIT COURT OF COOK COUNTY, ILLINOIS
COUNTY DEPARTMENT, CHANCERY DIVISION
GENERAL CHANCERY SECTION

PEOPLE OF THE STATE OF ILLINOIS, ex rel. Kimberly M. Foxx, State's Attorney of Cook County, Illinois, *Plaintiff,* v. FACEBOOK, INC., a Delaware corporation, SCL GROUP LIMITED, and CAMBRIDGE ANALYTICA, LLC, *Defendants.*	Case No. 2018 CH 03868 Calendar 03 Honorable Allen P. Walker

4680 4315
5271
4241

MEMORANDUM OF OPINION

This matter comes to be heard on Defendant, Facebook, Inc.'s, Motion to Dismiss Plaintiff's Complaint pursuant to 735 ILCS 5/2-301 and 735 ILCS 5/2-615 or, in the Alternative, Stay Proceedings pursuant to 735 ILCS 5/2-619(a)(3). The matter has been fully briefed and argued before the Court. Defendant Facebook, Inc.'s motion to dismiss pursuant to 735 ILCS 5/2-301 and 735 ILCS 2-615 regarding personal jurisdiction is denied. Facebook's motion to dismiss pursuant to 735 ILCS 5/2-619(a)(3) is denied. Defendant Facebook Inc.'s motion to dismiss pursuant to 735 ILCS 5/2-615 for failure to state a claim is granted without prejudice.

BACKGROUND

Plaintiff, the State of Illinois, brings this action under the Illinois Consumer Fraud and Deceptive Trade Practices Act (the "ICFA"), 815 ILCS 505, *et seq.* against Defendants, Facebook, Inc. ("Facebook"), and Cambridge Analytica, LLC ("Cambridge Analytica"), a data analytics company, for alleged misuse of Facebook users' sensitive personal information.

Facebook is a Delaware company, with its principal place of business in Menlo Park, California[1]. As of 2008, Facebook has been a registered business with the Illinois Secretary of State. First formed in 2004 as a friends' sharing website for college students, Facebook developed into a global online social media and social networking service with more than 2.3 billion monthly users worldwide. Facebook's online social networking platforms permit its users to publish and

[1]The facts recited herein are derived from Plaintiffs' Complaint and the exhibits attached thereto, and are accepted as true for purposes of Defendant's Motion to Dismiss. *Kedzie & 103rd Currency Exchange v. Hodge*, 156 Ill. 2d. 112, 115 (1993).

share personal information, from photos and videos to education and work histories, to political and religious affiliations. Users also share their "likes/dislikes" on a myriad of things.

Facebook's social networking platforms allows third-party ("3P") programmers to develop applications that can interface with other services and Facebook's online users. Through the Facebook Software Development Kit ("SDK"), 3P developers can add Facebook-related features to their applications, websites, or services. When 3P developers incorporate these features into their products, the developer's service can interact with Facebook and its users. A user must click through the appropriate permissions to allow the 3P's application to collect that user's and their *friends'* group data. Facebook also offers platforms for 3P advertisers and commercial content developers to market targeted online ads or programs to its users.

Defendant, Cambridge Analytica, LLC, is a Delaware limited liability company, organized with offices in Washington, D.C. and New York City. Established in 2013 as an entity within SCL Group (a UK private limited company), Cambridge is a political consulting firm that provides its customers with data analytics. In 2018, Cambridge Analytica offered to pay Facebook users to download and use a "personality quiz app" entitled *thisisyourdigitallife*. The app is alleged to have not only mined information about the user, but also the user's Facebook friends who had not agreed to use the app. Additionally, the data collected by Cambridge Analytica was allegedly used to create "psychographic profiles" for the 2016 United States presidential election, in which Cambridge Analytica obtained Facebook users' names, education, birthdays, and political tendencies.

On March 23, 2018, Plaintiff filed a three-count complaint (the "Complaint") against Defendants alleging: (1) a violation of the IFCA against Cambridge Analytica, Count I; (2) a violation of the IFCA by Facebook, Count II; and (3) entitlement to declaratory and injunctive relief, Count III. Plaintiff alleged that Facebook represented to its users that their personal data would be protected in accordance with its policies, when, in fact, it permitted third parties, such as Cambridge Analytica, to collect data despite its user agreements and misappropriate user information.

On April 19, 2019, Facebook filed a 2-619.1 motion to dismiss the Complaint. Facebook asserted, among other things, that it is not subject to personal jurisdiction in this Court. Following oral argument on the motion, the Court granted Plaintiff leave to amend the Complaint to cure any potential deficiencies. On October 3, 2019, Plaintiff filed its First Amended Complaint (the "FAC").

On October 31, 2019, Facebook filed a 2-619.1 motion to dismiss the FAC, this time with prejudice. This fully briefed motion is presently before the Court.

2-619.1 MOTION TO DISMISS STANDARD

A combined motion to dismiss pursuant to section 2-619.1 of the Illinois Code of Civil Procedure allows a party to combine a section 2-615 motion to dismiss based upon a plaintiff's substantially insufficient pleadings with a section 2-619 motion to dismiss based upon certain defects or defenses. 735 ILCS 5/2-619.1 (West 2018); *Illinois Non-Profit Risk Management Ass'n v. Human Service Center*, 378 Ill. App. 3d 713, 719 (4th Dist. 2008).

SECTION 2-619 STANDARD

Section 2-619 allows for disposal of issues of law or easily proved issues of fact. *Van Meter v. Darien Park District*, 207 Ill. 2d 359, 367 (2003). A section 2-619 motion admits all well-pleaded facts in the complaint but does not admit conclusions of law or conclusions of fact unsupported by specific allegations. *Better Government Ass'n v. Illinois High School Ass'n*, 2017 IL 121124, ¶ 21. "A section 2-619 motion admits the legal sufficiency of the complaint and raises defects, defenses, or other affirmative matter that appear on the face of the complaint or are established by external submissions that act to defeat the plaintiff's claim." *Hager v. II In One Contractors, Inc.*, 342 Ill. App. 3d 1082, 1086 (1st Dist. 2003). In reviewing a section 2-619 motion to dismiss, the court must construe all documents presented in the light most favorable to the non-moving party, and, if no disputed issue of material fact is found, the court should grant the motion. *Id.* However, if it cannot be determined with reasonable certainty that the defense exists, the motion to dismiss should be denied. *Saxon Mortgage. Inc. v. United Financial Mortgage. Corp.*, 312 Ill. App. 3d 1098, 1104 (1st Dist. 2000). A motion brought under 2-619 must satisfy a rigorous standard and can be granted only where "no set of facts can be proven that would support the plaintiff's cause of action." *Nosbaum v. Martini*, 312 Ill. App. 3d 108, 113 (1st Dist. 2000).

There are nine (9) enumerated bases for dismissal under section 2-619. 735 ILCS 5/2-619 (West 2018). Section 2-619(a)(3) of the Illinois Code of Civil Procedure provides that a "defendant may, within the time for pleading, file a motion for dismissal of the action *or for other appropriate relief* upon...[the fact] that there is another action pending between the same parties for the same cause." 735 ILCS 5/2-619(a)(3) (West 2014) (emphasis added). Other appropriate relief includes the issuance of a stay of a cause of action if "there is another action pending between the same parties for the same cause." *Id.* The movant bears the burden of establishing by clear and convincing evidence that the two actions involve the "same parties" and the "same cause." *Northbrook Property & Casualty Insurance Co. v. GEO International Corp.*, 317 Ill. App. 3d 78, 80 (1st Dist. 2000). Section 2-619(a)(3) is a procedural device designed to avoid duplicative litigation. *Quantum Chemical Corp. v. Hartford Steam Boiler Inspection & Insurance Co.*, 246 Ill. App 3d 557, 560 (3d Dist. 1993).

However, "even when the threshold requirements for 'same parties' and 'same cause' are met, Section 2-619(a)(3) relief is not mandatory." *Crain v. Lucent Technologies, Inc.*, 317 Ill. App. 3d 486, 495 (1st Dist. 2000). "Instead, the trial court has discretion to determine whether both actions should proceed through the weighing of several factors." *Schacht v. Lome*, 2016 IL App (1st) 141931, ¶ 34.

SECTION 2-615 STANDARD

A section 2-615 motion to dismiss, on the other hand, challenges the legal sufficiency of a complaint based on defects apparent on its face. *Marshall v. Burger King Corp.*, 222 Ill. 2d 422, 429 (2006). The motion does not raise affirmative factual defenses, but rather alleges only defects on the face of the complaint. *Beahringer v. Page*, 204 Ill. 2d 363, 369 (2003). The court must consider, in a light most favorable to the plaintiff, if the complaint is sufficient to state a cause of action upon which relief can be granted. *Id.* This determination requires an examination of the complaint as a whole, not its distinct parts. *Lloyd v. County of Du Page*, 303 Ill. App. 3d 544, 552 (2d Dist. 1999). In reviewing the sufficiency of a complaint, a court must accept all well-pleaded facts and all reasonable inferences that may be drawn from those facts. *Burger King Corp.*, 222 Ill. 2d at 429. A complaint is deficient when it fails to allege facts necessary for recovery. *Chandler v. Ill. Cent. R. R.*, 207 Ill. 2d 331, 348 (2003). A court should not dismiss a cause of action unless it is clearly apparent that no set of facts can be proven that would entitle the plaintiff to recovery. *Redelmann v. Claire Sprayway, Inc.*, 375 Ill. App. 3d 912, 921 (1st Dist. 2007).

DISCUSSION

As a preliminary matter, the Court notes that Facebook seeks dismissal pursuant to 735 ILCS 5/2-301 and 2-615, arguing that it is not subject to specific personal jurisdiction in this Court. Plaintiff counters that Facebook waived its personal jurisdiction claim by (1) filing for a substitution of judge as of right pursuant to 735 ILCS 5/2-1001(a)(2) prior to filing their motion to dismiss, and (2) seeking a stay in federal court after Facebook previously removed the case. As such, the Court deems it necessary to first address Plaintiff's arguments regarding the waiver issue.

I. Dismissal Pursuant to Section 2-301 and 2-615 – Waiver of Personal Jurisdiction

Plaintiff argues that Facebook twice waived its challenge to the Court's exercise of personal jurisdiction by: (1) filing for a substitution of judge as of right prior to filing their motion to dismiss, and (2) seeking a stay in federal court after Facebook previously removed the case.

First, Plaintiff contends that Facebook's decision to file a motion for substitution of judge as of right prior to the motion to dismiss was improper. According to Plaintiff, 735 ILCS 5/2-301(a-6) requires a party to raise an objection to personal jurisdiction before filing "any other . . . motion." Moreover, Plaintiff asserts that while Section 301(a-6) articulates certain exceptions to this general rule, there is no exception for a motion for substitution of judge pursuant to 735 ILCS 5/2 1001(a)(2). As such, Plaintiff insists that Facebook waived its opportunity to object to personal jurisdiction when it failed to simultaneously assert its objection when it filed its motion for substitution of judge.

Next, Plaintiff argues that Facebook's request for a stay in federal court constitutes another example of a "motion" Facebook filed prior to its motion to dismiss where it asserted its personal jurisdiction defense. Accordingly, Plaintiff contends that Facebook's failure to raise objections to

personal jurisdiction concurrently or before the motion to dismiss resulted in a type of forum shopping that 735 ILCS 5/2-301(a-6) was meant to prevent.

Facebook responds that Plaintiff asserted its arguments regarding waiver for the first time in Plaintiff's response to Facebook's second motion to dismiss. By failing to raise the waiver arguments in opposition to Facebook's first motion to dismiss, Facebook contends Plaintiff's arguments are waived. Additionally, Facebook argues it did not waive its challenge to this Court's exercise of personal jurisdiction because the motion for substitution of judge was *pro forma*. Further, Facebook points out that Plaintiffs fail to cite any authority to support their position, and thus, Facebook should not be forced to relinquish its statutory right in order to proceed with its objections.

Regarding Plaintiff's argument that Facebook's request for a stay in federal court constituted a waiver of any objections to personal jurisdiction, Facebook asserts that under Fed. R. Civ. P. 12(h)(1), personal jurisdiction is waived only if a defendant fails to raise the defense in their initial motion to dismiss or responsive pleading. Moreover, Facebook argues merely seeking to stay litigation in federal court does "not waive [the] defense of lack of personal jurisdiction," citing *Lane v. XYZ Venture Partners, LLC*, 322 F. App'x 675, 678 (11th Cir. 2009).

This Court finds that Facebook waived its challenge to personal jurisdiction by filing a motion for substitution of judge pursuant to 735 ILCS 5/2-1001(a)(2). The language pursuant to 735 ILCS 5/2-301(a-6) clearly states:

> A party filing *any other* pleading *or motion* prior to the filing of a motion objecting to the court's jurisdiction over the party's person as set forth in subsection (a) *waives all objections to the court's jurisdiction over the party's person* prospectively, unless the initial motion filed is one of the following:
>
> **(1)** A motion for an extension of time to answer or otherwise plead; or
> **(2)** A motion filed under Section 2-1301, 2-1401, or 2-1401.1

735 ILCS 5/2-301(a-6) (West 2018) (emphasis added).

The Court agrees with Plaintiff that a motion for substitution for judge as of right is, in fact, a motion pursuant to 735 ILCS 5/2-1001(a)(2) that is not provided for in the exceptions to 735 ILCS 5/2-301. If the party objecting to jurisdiction files a motion outside the exceptions listed in 735 ILCS 5/2 301(a-6), then the party waives all objections to the court's jurisdiction over that party. See *Resurgence Capital, LLC v. Kuznar*, 2017 IL App (1st) 161853, ¶ 1.

When construing a statute, our primary objective is to ascertain and give effect to the intent of the legislature. *People v. Elliott*, 2014 IL 115308, ¶ 11. "The most reliable indicator of legislative intent is the statutory language, given its plain and ordinary meaning." *BAC Home Loans Servicing, LP v. Mitchell*, 2014 IL 116311, ¶ 33. While Facebook argues that a motion for

substitution of judge pursuant to 735 ILCS 5/2-1001(a)(2) is merely *pro forma*, the plain and ordinary language of 735 ILCS 5/2-301(a-6) provides no caveats for such *pro forma* motions. Rather, the plain and ordinary language in 735 ILCS 5/2-301(a-6) reveals no other exceptions except for the listed motions within it. If the legislature meant to exempt motions for substitution of judge as of right, then it certainly could have added 735 ILCS 5/2-1001(a)(2) to the list in 735 ILCS 5/2-301(a-6), but it did not do so. This Court recognizes the long-standing practice of finding that filing a motion not listed in 735 ILCS 5/2-301 before any jurisdictional issues are raised as constituting waiver of such jurisdictional issues. See generally *BAC Home Loans Servicing*, 2014 IL 116311 at ¶ 37 (there is a "long-standing rule that a party may waive a defect in jurisdiction over the person by proceeding without objection.").

In *Resurgence Capital*, the defendant had filed a petition for sanctions, a motion for substitution of judge as of right, a reply to the plaintiff's response to the petition for sanctions, a petition for discovery, and an objection to and request to strike the plaintiff's sur-reply to the petition for sanctions all before he filed a motion to dismiss. *Resurgence Capital, LLC v. Kuznar*, 2017 IL App (1st) 161853, ¶ 24. While his motion to dismiss was based on insufficiency of service of process and ultimately a lack of personal jurisdiction, the court in *Resurgence Capital* determined the defendant had waived all personal jurisdiction pursuant to the plain terms of 735 ILCS 5/2-301(a) and (a-5) by previously filing such motions.[2] *Id.* While the defendant in *Resurgence* Capital filed many more motions before raising its objections to personal jurisdiction than Facebook has done in the present case, the Illinois Appellate Court still recognized in *Resurgence Capital* that a motion for substitution of judge as of right is among those motions that will waive personal jurisdiction objections if filed prior to raising of such personal jurisdiction objections. *Id.*

Here, it is true that Facebook merely filed a singular motion—motion for substitution of judge as of right—prior to filing its motion dismiss containing personal jurisdiction objections. However, Facebook, in the filing of that motion, consented to this Court's jurisdiction according to 735 ILCS 5/2-301(a-6).

The Court notes that Facebook filed its motion for substitution of judge as of right on April 12, 2019. Facebook then filed its motion to dismiss the complaint, asserting its personal jurisdiction objection for the first time, on April 19, 2019. Facebook could have filed its motion for substitution of judge as of right concurrently with its motion to dismiss, but instead filed its motion to dismiss seven (7) days after it had filed its motion for substitution of judge as of right. Alternatively, Facebook could have filed a motion for substitution of judge as of right *after* it objected to personal jurisdiction in its motion to dismiss. Because Facebook failed to utilize either of these options, the Court finds that it waived its objections to personal jurisdiction.

---

[2] When the *Resurgence Capital* decision was issued, 735 ILCS 5/2-301 was worded slightly differently from the current version of the same statute applicable today; however, it read in a substantially similar way as it stated the following: "If the objecting party files a responsive pleading or a motion (other than a motion for an extension of time to answer or otherwise appear) prior to the filing of a motion in compliance with subsection (a), that party waives all objections to the court's jurisdiction over the party's person." 735 ILCS 5/2-301(a-5) (LexisNexis 2016).

Additionally, the Court finds that the question of whether Plaintiff should have presented this argument in response to Facebook's first motion to dismiss is immaterial. Plaintiff presented its waiver argument in response to Facebook's second motion to dismiss, which is presently before this Court. Moreover, Facebook fails to cite any authority to support its position that a party may not subsequently assert a waiver argument if it did not assert the argument in a prior motion to dismiss an earlier complaint.

Lastly, because this Court finds that Facebook has waived its personal jurisdiction objections by filing its motion for substitution of judge as of right, this Court need not address the alleged waiver of personal jurisdiction through Facebook's filing of a stay in federal court after it removed the case. Accordingly, this Court finds that it has personal jurisdiction over Facebook in this matter.

Having addressed the overarching jurisdictional issue, the Court now turns to Facebook's arguments for dismissal pursuant to Section 2-615 for failure to state a claim.

II. Dismissal Pursuant to Section 2-615 - Failure to State a Claim Under ICFA

Facebook argues that this Court should dismiss Plaintiff's FAC pursuant to 735 ILCS 5/2-615 because Plaintiffs fail to state a claim under the ICFA. According to Facebook, to establish an ICFA claim, Plaintiff had to allege: "(1) a deceptive act or promise by the defendant; (2) the defendant's intent that the plaintiff rely on that act or promise; and (3) that the deception occurred during a course of conduct involving trade or commerce," citing *People ex rel. Madigan v. United Constr. of Am., Inc.*, 2012 IL App (1st) 120308, ¶ 16. Facebook notes that Plaintiff's FAC fails to satisfy the first prong of an ICFA claim. Facebook contends an ICFA fails when consumers "kn[o]w the truth," citing *Oliveira v. Amoco Oil Co.*, 201 Ill.2d 134, 155 (2002). Facebook argues that "full and accurate disclosure" cannot "conceal, suppress, or hide any material facts," citing *Krause v. GE Capital Mortg. Serv., Inc.*, 314 Ill. App. 3d 376, 388 (1st Dist. 2000).

Facebook argues that its Data Use Policy accurately informed its users of the data-sharing process:

> Just like when you share information by email or elsewhere on the web, information you share on Facebook can be re-shared. This means that if you share something on Facebook, anyone who can see it can share it with others, including the games, applications, and websites they use. . . . If you have made [particular] information public, then the application can access [that information] just like anyone else.

Ex. 2 at 40.

Accordingly, Facebook insists that it did not deceive its users because they were made aware of its Data Use Policy. Moreover, absent specific allegations by Plaintiff as to what is misleading about Facebook's statements regarding user control over data-sharing with apps, Facebook contends there is no ICFA claim.

Moreover, Facebook notes that Plaintiff's FAC alleges that Facebook shared with users its policies that: (1) third-party applications may "not directly or indirectly transfer any data [they] receive from [Facebook] to (or use such data in connection with) any ad network, ad exchange, data broker, or other advertising related toolset, even if a user consents to that transfer or use," and (2) that applications use user information "only in connection with the person that gave the permission [to access the information], and no one else." FAC at ¶¶ 50, 53. However, Facebook contends that these statements *do* accurately inform users about the contractual obligations that third-party app developers assume, and highlights that Facebook made no guarantee that such third-party app developers would not somehow violate those policies.

While the FAC alleges that Facebook mislead users about how it would monitor third-party applications, Facebook argues that it never promised to control the actions of third parties through audits or other limitations. Facebook asserts that an ICFA claim is not "cognizable . . . in the absence of any claimed affirmative misstatement," citing *Phillips v. DePaul Univ.*, 2014 IL App (1st) 122817, ¶ 40. Facebook contends that the Plaintiff "has not pled that Facebook *lacked the ability to* require applications to delete data, limited applications' access to data, or audited applications . . . Facebook *did* avail itself of these tools." Mot. at ¶ 13.

Further, Facebook argues that the FAC's allegation regarding Facebook's failure to inform users of the Cambridge Analytica events also does not state an ICFA claim. Facebook emphasizes that the events regarding Cambridge Analytica's actions were made public in 2015 via an article by the Guardian and that no one was actually deceived as a result of the omission. Facebook additionally argues that the Personal Information Protection Act ("PIPA"), 815 ILCS 530/1, would be the relevant statute under which to bring a claim, as it is more specific than the ICFA and controls when data breaches need to be disclosed. Because the Plaintiff has not alleged violations under PIPA, Facebook argues the Plaintiff should not be allowed to allege data breach claims under the more generalized provisions of ICFA.

Plaintiff responds by arguing that they have sufficiently pled a violation of the ICFA because they have alleged that Facebook's users did not know that Cambridge Analytica had exfiltrated their data. Plaintiff points out that the FAC states that that "Cambridge Analytica's business practices were largely a secret to the general public." FAC at ¶ 60. While acknowledging that the Guardian's article did cover the incident in 2015, Plaintiff asserts that it is not reasonable to assume that such article would put every affected Facebook user on notice of the incident. Plaintiff refers to the swarm of coverage that took place in 2018 after lawsuits regarding the incident began to take place, resulting in Facebook's Mark Zuckerberg's public apology for breaching user trust.

Plaintiff additionally argues that PIPA is not the applicable statute in this instance. Although Plaintiff agrees that the more specific statute should apply where two statutes are applicable, Plaintiff contends that PIPA is *not applicable*. Plaintiff also argues that the ICFA and PIPA are not in conflict, and because the ICFA is the applicable statute, the Illinois Supreme Court has determined the ICFA is to be liberally construed. Plaintiff, citing *Aliano v. Ferriss*, 2013 IL App (1st) 120242, ¶ 24, argues the FAC need only show that Facebook's statements as a whole give the impression of being misleading. However, maintaining its position that Facebook's statements *individually* are misleading, Plaintiff quotes language from Facebook's Data Use Policy that was stated in the FAC:

> If you are a developer or operator of a Platform application or website, the following additional terms apply to you:
> You [developers] will only request data you need to operate your application. . .
> You will not directly or indirectly transfer any data you receive from us to (or use such data in connection with) any ad network, ad exchange, data broker, or other advertising related toolset, even if a user consents to that transfer or use.
> You will not sell user data. . .
> We can require you to delete user data if you use it in a way that we determine is inconsistent with users' expectations.
> We can limit your access to data. . .
> To ensure your application is safe for users, we can audit it

FAC at ¶ 50.

According to Plaintiff, these statements show user privacy settings would not control how their data was shared once in the hands of third-party app developers. According to Plaintiff, these statements give the impression that Facebook would take further steps to exercise enforcement powers. Plaintiff reiterates that facts are to be taken in the light most favorable to it, and therefore, it is reasonable to conclude that an ordinary Facebook user would understand Facebook's disclosures would keep such user's data safe from third-party app developers.

Facebook replies that PIPA is the applicable statute because PIPA lays out specific circumstances in which companies are to notify Illinois residents in the case of a data breach. Facebook reads the FAC as supporting the theory of the case that a data breach occurred, as it refers to Cambridge Analytica's acquisition of user data as a "breach." FAC at ¶¶ 6, 104, 127. If such a data breach occurred, Facebook contends that Plaintiff should bring its alleged claim under PIPA and not ICFA, which is the more general consumer statute.

In terms of Plaintiff's misrepresentation claim, Facebook emphasizes that the FAC's allegations still do not allege an intent to deceive its users. While Facebook acknowledges the FAC states that Facebook's "statements were intended to deceive," this statement is not supported by any factual allegations to support it. Instead, Facebook contends this statement is conclusory. Facebook points out that Plaintiff concedes that Facebook's statements are not facially false, but rather, merely attempts to argue that the "net impression" of the statements allegedly reveal they

are misleading. Facebook refutes Plaintiff's reading of *Aliano*, because in that case, the "net impression" test was used exclusively in interpretating advertisement representations. Facebook contends that the "net impression" test has not ever been used outside of this context, citing *Schreib v. Walt Disney Co.*, 2006 WL 573008, at *3 (Ill. App. Ct. Feb. 1, 2006) and *Garcia v. Overland Bond & Inv. Co.*, 282 Ill. App. 3d 486, 491 (1st Dist. 1996). Additionally, Facebook contends that it instructed its users on how to secure their data via its application settings, and that it in no way guaranteed that it would take any particular action against third-party app developers who ultimately misused user data. Regardless, Facebook argues that it did, in fact, take action against Cambridge Analytica by requiring Cambridge Analytica to verify that it deleted user data.

This Court will first address whether the Plaintiff's allegations have been brought under the proper statute. While Facebook reads the FAC as alleging a data breach occurred, the FAC's allegations are focused on Facebook's alleged misrepresentations to its users. This Court agrees with Plaintiff that PIPA and ICFA are not in conflict, and, as PIPA is not applicable to Plaintiff's allegations, the ICFA is the applicable statute. While the Illinois Supreme Court has reiterated that the ICFA was not intended to apply to fraudulent actions that take place outside of Illinois, the ICFA itself does not contain any geographic limitations. See *Avery v. State Farm Mut. Auto. Ins. Co.*, 216 Ill. 2d 100, 181 (2005). Plaintiff's FAC does not state any facts that show Facebook's alleged misrepresentations occurred specifically in Illinois and instead relies on its assertions that those misrepresentations affected residents in Illinois. While Plaintiff does not show how Illinois residents were *uniquely* affected in comparison to other citizens throughout the country, the FAC does at least allege that Illinois residents suffered harm due to Facebook's actions. Therefore, this Court finds that Plaintiff properly brought its allegations under the ICFA.

At the motion to dismiss stage, under 735 ILCS 5/2-615, a court should not dismiss a cause of action unless it is clearly apparent that no set of facts can be proven that would entitle the plaintiff to recovery. *Redelmann*, 375 Ill. App. 3d at 921. Under the ICFA, Illinois law provides that the elements of a claim for consumer fraud are: (1) a deceptive act or practice by the defendant; (2) the defendant's intent that the plaintiff rely on the deception; and (3) that the deception occurred in the course of conduct involving trade and commerce. *Connick*, 174 Ill. 2d at 501; 815 ILCS 505/10(a) (West 2012). While Plaintiff attempts to argue that the FAC need only provide this Court with a "net impression" that Facebook made misrepresentations to its users, case law indicates otherwise. Facebook correctly distinguishes the "net impression" test in *Aliano*, the only case cited by Plaintiff in support of this argument, as being primarily used in evaluating advertising representations. In *Aliano*, the court stated that "[i]t is well established that ***the test to be used in interpreting advertising*** is the net impression that it is likely to make on the general populace." *Aliano*, 2013 IL App (1st) 120242 at ¶ 24 (emphasis added). Other cases employing the net impression test have done so in the context of claims involving representations in advertisements. *Williams v. Bruno Appliance & Furniture Mart, Inc.*, 62 Ill. App. 3d 219, 219 (1978) (plaintiff consumer brought suit against defendant alleging defendant violated the Consumer Fraud and Deceptive Practices Act by engaging in false advertising); *Garcia v. Overland Bond & Inv. Co.*, 282 Ill. App. 3d 486, 488 (1996) (plaintiff brought an ICFA claim against a car dealer with allegations that he advertised and sold defective cars); *People ex rel. Hartigan v. Maclean Hunter Publ'g Corp.*, 119 Ill. App. 3d 1049, 1051 (1983) (plaintiff brought

ICFA claim based on publisher's advertisements of vehicle pricing manual). The Court finds that Plaintiff's FAC merely provides Facebook's policies as evidence of misrepresentation and Plaintiff has not sufficiently alleged that Facebook *advertised* in any specific way that it would guarantee the safety of user data. Therefore, in this instance, the net impression test is not applicable.

The FAC states that "Facebook represented to its Illinois users that their personal data would be protected in accordance with its SRR and Data Use Policies. . ." FAC at ¶ 123. While the Plaintiff points to language in Facebook's User Policy and Data Use Policy, Plaintiff concedes that these statements are not facially false. Facebook's Data Use Policy consistently includes language such as "can" and "we determine" that implies a permissive option for Facebook to take––not a mandatory action that is laid out. Whether or not these statements are facially false is separate from whether these statements could be used to deceive users into believing that their data was completely safe.

This Court finds that FAC as it currently stand does not provide a plausible basis to coclude that a reasonable person reading these policies might believe that their data was guaranteed to be safe from third-party app developers, especially third-party developers who might violate Facebook's Data Use Policy. Instead, Facebook repeatedly states in its policies that it is not responsible for the actions of third parties and thus when the FAC states that "those statements were intended to deceive consumers," the Court is not provided with further facts on how that would be the case. While the FAC states that Facebook "did essentially nothing" to investigate, it does not allege that Facebook has a duty to do more than it has done. Facebook's relevant policies only indicate the enforcement available to it and Facebook makes no guarantee as to how it will proceed in such investigations. The FAC acknowledges that Facebook did, in fact, use its enforcement against Cambridge Analytica by requiring that Cambridge Analytica delete its acquired data. That action was specifically laid out in the Data Use Policy that allowed Facebook to "delete user data if [used] in a way that [Facebook] determine[s] is inconsistent with users' expectations." FAC at ¶ 50.

Further, the FAC fails establish the second element of an ICFA claim, namely that Facebook intended for its users to rely on any alleged misrepresentations. A complaint alleging a violation of Consumer Fraud Act must be pled with the same specificity as that required under common law fraud." *Id.* Here, while the FAC alleges that Facebook's statements "intended to deceive consumers," Plaintiff does not state facts that support that allegation. Indeed, Plaintiff acknowledges that it was Cambridge Analytica who "intentionally violated Facebook's policies," which begs the question of how Facebook could have intended to deceive its users when it was itself was deceived. FAC at ¶ 103. In fact, this action by Facebook seems to contradict that Facebook intended to deceive users. Facebook's policies were clearly violated by Cambridge Analytica, which was admitted to in the FAC, and thus the FAC is contradictory when alleging that Facebook "permitted third parties, including Cambridge Analytica, to collect and harvest its user's personal data. . ." FAC at ¶ 125. By having a policy in place, Facebook could not intend for Cambridge Analytic to violate it. Thus, the FAC fails to set forth allegations that Facebook intended that its users would rely on the alleged misrepresentations.

As Plaintiff's FAC fails to sufficiently plead (1) a deceptive act or promise by Facebook, and (2) that Facebook intended for its users to rely on any deceptive act or promise, the Court finds that Plaintiff has failed to state a cause of action under the ICFA. Accordingly, the Court grants Facebook's motion to dismiss pursuant to Section 2-615 without prejudice. Moreover, having granted Facebook's motion pursuant to 2-615, the Court denies Facebook's 2-619(a)(3) request to stay proceedings in light of actions pending elsewhere.

CONCLUSION

Defendant, Facebook, Inc.'s, motion to dismiss pursuant to 735 ILCS 5/2-301 and 735 ILCS 5/2-615 regarding personal jurisdiction is denied. Facebook's motion to dismiss pursuant to 735 ILCS 5/2-619(a)(3) is denied. Defendant Facebook Inc.'s motion to dismiss pursuant to 735 ILCS 5/2-615 for failure to state a claim is granted without prejudice. This matter is set for status on April 20, 2021 at 10:00am.

Allen Price Walker
ENTERED:
Associate Judge

Mar. 08, 2021

Circuit Court - 2071
Allen P. Walker

DATED: March 2, 2021

District of Columbia
Court of Appeals

REDACTION CERTIFICATE DISCLOSURE FORM

Pursuant to Administrative Order No. M-274-21 (filed June 17, 2021), this certificate must be filed in conjunction with all briefs submitted in all cases designated with a "CV" docketing number to include Civil I, Collections, Contracts, General Civil, Landlord and Tenant, Liens, Malpractice, Merit Personnel, Other Civil, Property, Real Property, Torts and Vehicle Cases.

I certify that I have reviewed the guidelines outlined in Administrative Order No. M-274-21 and Super. Ct. Civ. R. 5.2, and removed the following information from my brief:

1. All information listed in Super. Ct. Civ. R. 5.2(a); including:

   - An individual's social-security number
   - Taxpayer-identification number
   - Driver's license or non-driver's' license identification card number
   - Birth date
   - The name of an individual known to be a minor
   - Financial account numbers, except that a party or nonparty making the filing may include the following:

     (1) the acronym "SS#" where the individual's social-security number would have been included;
     (2) the acronym "TID#" where the individual's taxpayer-identification number would have been included;
     (3) the acronym "DL#" or "NDL#" where the individual's driver's license or non-driver's license identification card number would have been included;
     (4) the year of the individual's birth;
     (5) the minor's initials; and
     (6) the last four digits of the financial-account number.

2. Any information revealing the identity of an individual receiving mental-health services.

3. Any information revealing the identity of an individual receiving or under evaluation for substance-use-disorder services.

4. Information about protection orders, restraining orders, and injunctions that "would be likely to publicly reveal the identity or location of the protected party," 18 U.S.C. § 2265(d)(3) (prohibiting public disclosure on the internet of such information); *see also* 18 U.S.C. § 2266(5) (defining "protection order" to include, among other things, civil and criminal orders for the purpose of preventing violent or threatening acts, harassment, sexual violence, contact, communication, or proximity) (both provisions attached).

5. Any names of victims of sexual offenses except the brief may use initials when referring to victims of sexual offenses.

6. Any other information required by law to be kept confidential or protected from public disclosure.

/s/ Jeremy R. Girton
Signature

23-CV-550
Case Number(s)

Jeremy R. Girton
Name

3/29/2024
Date

jeremy.girton@dc.gov
Email Address

Public Version

CERTIFICATE OF SERVICE

I certify that on March 29, 2024, this corrected brief was served through this Court's electronic filing system to:

Joshua S. Lipshutz
Helgi Walker
Katherine Moran Meeks

/s/ Jeremy R. Girton
JEREMY R. GIRTON