U.S. COURT OF APPEALS FOR THE THIRD CIRCUIT

No. 23-3235

IN RE: BPS DIRECT, LLC; CABELA'S, LLC WIRETAPPING LITIGATION

BRIAN CALVERT; HEATHER CORNELL; TIMOTHY DURHAM; MARILYN HERNANDEZ; GREG MOORE, JR.; ET AL.,
Appellants

Appeal from the U.S. District Court, E.D. Pa.
Judge Mark A. Kearney,
Nos. 2:23-md-03074, 2:22-cv-04709, 2:23-cv-02282, 2:23-cv-02287, 2:23-cv-02293, 2:23-cv-02294, 2:23-cv-02295, 2:23-cv-02306, 2:23-cv-02338 & 2:23-cv-04008

Before: HARDIMAN, KRAUSE, and FREEMAN, *Circuit Judges*
Argued Sep. 10, 2025; Decided May 11, 2026

OPINION OF THE COURT

FREEMAN, *Circuit Judge*.

Outdoor products retailers Bass Pro Shops and Cabela's (collectively, "BPS") use a JavaScript computer code known as "Session Replay Code" on their websites. The Session Replay Code captures and stores users' interactions on the websites, including mouse movements, text entries, and clicks.

In a putative class action, eight named plaintiffs claimed that BPS's use of Session Replay Code without their consent violated various state and federal privacy laws. The District Court dismissed the complaint for lack of Article III standing.

The plaintiffs allege intangible injuries, so to demonstrate standing they must assert injuries that have a "close relationship" to a harm traditionally recognized at common law. *TransUnion LLC v. Ramirez*, 594 U.S. 413, 417 (2021) (quoting *Spokeo, Inc. v. Robins*, 578 U.S. 330, 340–41

(2016)). Because two plaintiffs have done so, we will REVERSE the dismissal order as to them and REMAND for further proceedings.

The District Court properly dismissed the claims of the remaining six plaintiffs. But dismissals for lack of standing should be without prejudice, so we will MODIFY the order to make it a dismissal without prejudice as to those plaintiffs, and we will AFFIRM that part of the order as modified.

I[1]

BPS procures Session Replay Code developed by various third-party Session Replay Code providers ("Providers"), such as Microsoft, Quantum Metric, and Mouseflow. BPS embeds that code on its retail websites: www.basspro.com and www.cabelas.com. The code activates anytime a user visits one of these websites, allowing it to surreptitiously intercept nearly every action a user takes on the site, including "all mouse movements, clicks, scrolls, zooms, window resizes, keystrokes, [and] text entries." App. 88.

The Session Replay Code intercepts this data with hyper-frequency, in intervals just milliseconds apart. Thus, it captures inputs that a user types into text fields even if the user does not click "submit" or "enter" on the website. BPS and the Providers can then use the data captured by the Session Replay Code to create "video replay[s]" of website users' visits to BPS's websites. App. 69. Those video replays give BPS insights into the performance of its websites and its advertising campaigns.

[1] We accept the facts alleged in the complaint as true and construe them in the light most favorable to the plaintiffs. *Barclift v. Keystone Credit Servs., LLC*, 93 F.4th 136, 141 (3d Cir. 2024). Although we also discussed Session Replay Code in our opinion in *Cook v. GameStop, Inc.*, 148 F.4th 153 (3d Cir. 2025), our description of the technology here is based on the allegations in this case's complaint.

The third-party Providers also store data collected from users of BPS's websites on their own servers. These data include personally identifying information.

The Providers can (and often do) aggregate and store users' data under identifiers called "fingerprints." "Fingerprints" are unique to a particular user's combination of computer and browser settings and other detectable information. Each Provider can collect "fingerprints" across all websites that use their Session Replay Code—not just websites owned by BPS. If a user identifies herself on one of these websites (by filling out a form, for example), a Provider can match that user's "fingerprint" with her identity. That Provider can then connect that user's identity with her prior web browsing activity from sites that use the same Provider's Session Replay Code, including from websites where the user intended to remain anonymous by, for instance, enabling private browsing.

BPS does not give users an opportunity to opt out of its use of the Session Replay Code on its websites. In fact, typical users navigating BPS's websites through a standard browser's default view do not even know the Session Replay Code is embedded in those sites. Only users with website-programmer skills can deploy the technical tools needed to see the underlying Session Replay Code, and even those skilled users would need to know what to look for.

In federal district courts across the country, eight individuals sued BPS for its use of Session Replay Code. Those cases were transferred to the Eastern District of Pennsylvania, and the eight plaintiffs then filed a consolidated class action complaint. All eight plaintiffs seek relief because BPS's use of Session Replay Code captured their interactions on BPS's websites, including "mouse clicks and movements, keystrokes, search terms, substantive information inputted . . . , pages and content viewed . . . , scroll movement[s], and copy and paste actions." App. 99. They claim that BPS violated two federal statutes—the Wiretap Act, 18 U.S.C. § 2510 *et seq*., and the Computer Fraud and Abuse Act, *id.* § 1030 *et seq*.—and is also liable under several state and common-law causes of action.

According to the consolidated complaint, two plaintiffs—Heather Cornell and Peter Montecalvo—made purchases after browsing on a BPS website. Cornell purchased a camp chair on www.basspro.com, and Montecalvo bought a belt and other items during multiple visits to www.cabelas.com. During their respective checkout processes, Cornell and Montecalvo each entered his or her "name, address, and payment and billing information" into text fields. App. 100, 103.

The remaining six plaintiffs—Brian Calvert, Timothy Durham, Marilyn Hernandez, Greg Moore, Arlie Tucker, and Brittany Vonbergen—browsed for items on BPS's websites but made no purchases.[2] They did not enter their names, addresses, or any other personally identifying information while on the websites.

BPS moved to dismiss the complaint under Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6). The District Court granted the motion under Rule 12(b)(1), concluding that none of the plaintiffs demonstrated Article III standing. It reasoned that the "website users must be able to plead facts of sharing highly sensitive personal information such as a medical diagnosis or financial data from banks or credit cards to enjoy Article III standing." *In re BPS Direct, LLC*, 705 F. Supp. 3d 333, 367 (E.D. Pa. 2023). Because the six plaintiffs who did not make purchases on BPS's websites had two chances to allege these facts, the District Court dismissed their claims with prejudice.

Because Cornell and Montecalvo made purchases on a BPS website, the District Court dismissed their claims "without prejudice to their timely filing amended Complaints if they can truthfully allege [BPS] intercepted and shared highly sensitive personal information such as medical diagnosis information or financial data from banks or credit

[2] Durham alleged that he accessed www.cabelas.com, but he provided no details about when he accessed that website or what actions he took while there. For simplicity, and despite his deficient pleading, we address Durham's claims alongside those from the plaintiffs who browsed BPS websites but made no purchases.

cards . . . during their interactions (including the alleged purchase[s]) on the website." *Id.* at 367. Rather than amending, Cornell and Montecalvo filed a notice of their intent to stand on the allegations in the consolidated complaint.

All eight plaintiffs timely appealed.

II[3]

We review de novo a district court's order dismissing a complaint pursuant to Federal Rule of Civil Procedure 12(b)(1). *In re Horizon Healthcare Servs. Inc. Data Breach Litig.*, 846 F.3d 625, 632 (3d Cir. 2017). In doing so, "we consider whether the complaint 'contain[s] sufficient factual matter that would establish standing if accepted as true.'" *Potter v. Cozen & O'Connor*, 46 F.4th 148, 153 (3d Cir. 2022) (citation modified).

A

"Standing is an irreducible constitutional minimum." *Road-Con, Inc. v. City of Philadelphia*, 120 F.4th 346, 354 (3d Cir. 2024) (citation modified). To establish standing, a "plaintiff must have (1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision." *Cook v. GameStop, Inc.*, 148 F.4th 153, 157 (3d Cir. 2025) (quoting *Spokeo*, 578 U.S. at 338). Plaintiffs bear the burden of establishing these elements, *id.*, and each plaintiff in a multi-plaintiff action must demonstrate standing, *see TransUnion*, 594 U.S. at 431.

Only the first element of standing—injury in fact—is contested here. "To establish injury in fact, a plaintiff must show that he or she suffered an invasion of a legally protected interest that is concrete and particularized and actual or imminent, not conjectural or hypothetical." *Spokeo*, 578 U.S. at 339 (citation modified). To be "concrete" an injury must be

[3] The District Court had jurisdiction under 28 U.S.C. §§ 1331 and 1332(d)(2)(A). We have jurisdiction under 28 U.S.C. § 1291.

"real, and not abstract." *TransUnion*, 594 U.S. at 424 (citation modified).

The "most obvious" concrete injuries result from "traditional tangible harms, such as physical harms and monetary harms." *Id*. at 425. But certain intangible harms also give rise to concrete injuries. "Chief among them are injuries with a close relationship to harms traditionally recognized as providing a basis for lawsuits in American courts." *Id.* So when plaintiffs allege an intangible harm, we ask whether they "have identified a close historical or common-law analogue for their asserted injury." *Id.* at 424. We do so by "compar[ing] the kind of harm a plaintiff alleges with the kind of harm caused by [a] comparator tort" at common law. *Barclift*, 93 F.4th at 144–45; *GameStop*, 148 F.4th at 158–59.

The plaintiffs here argue that their injuries are analogous to the harms recognized by two common-law torts: (1) public disclosure of private facts and (2) intrusion upon seclusion. As explained below, no plaintiffs have alleged injuries analogous to those caused by a public disclosure of private facts, and only Montecalvo and Cornell have alleged injuries analogous to those caused by an intrusion upon seclusion.

B

The tort of public disclosure of private facts is also known as "unreasonable publicity given to another's private life." *Barclift*, 93 F.4th at 145. A defendant is liable for this tort if he "gives publicity to a matter concerning the private life of another . . . if the matter publicized is one of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public." Restatement (Second) of Torts § 652D (1977) ("Second Restatement § 652D"). The harm is "the humiliation that accompanies the disclosure of sensitive or scandalizing private information to public scrutiny." *Barclift*, 93 F.4th at 145–46 (citation modified). So if the information disclosed is not of an "offensive character," or if the information is not disclosed to the public, the harm is not analogous. *Id.* at 146.

In *Barclift v. Keystone Credit Services*, Barclift alleged that a credit servicing company shared her personal

information absent authorization with a third-party mailing vendor, which then mailed the company's collection notice to her. *Id.* at 139. She argued that her injury was analogous to the harm caused by the tort of public disclosure of private facts. *See id.* at 145–46.[4] We disagreed. Barclift did not allege that the credit servicing company shared her personal information with anyone other than its mailing vendor, which was "a single ministerial intermediary." *Id.* at 146 (citation modified). Because the information "remain[ed] functionally internal," Barclift did not suffer the kind of harm associated with the comparator tort. *Id.* So for Article III purposes, her injury was not concrete.

We reached a similar conclusion recently in a case involving Session Replay Code. In *Cook v. GameStop*, Cook alleged that the retailer GameStop used Session Replay Code to capture her interactions on its website and aggregate that data into a video that recreated her visit. *See* 148 F.4th at 156. The code captured Cook's mouse movements, the links she clicked, her text entries, and other actions she took while browsing GameStop's website. *Id.* at 156, 159. But Cook did not enter (so the code did not capture) "her name, contact information, address, or billing information while on [the] website." *Id.* at 159.[5] Because the code did not capture any of Cook's sensitive or personal information, any injury she suffered was not analogous to "the humiliation that accompanies the disclosure of sensitive or scandalizing private information to public scrutiny." *Id.* at 159 (quoting *Barclift,* 93 F.4th at 145–46). So we held that Cook did not suffer a concrete injury.

---

[4] Unlike plaintiffs here, Barclift did not analogize her injury to that caused by the tort of intrusion upon seclusion.

[5] Cook alleged that the Session Replay Code created a profile of her based on information obtained from her device and browser, but her identity was not part of that information. 148 F.4th at 160. That is, she "alleged only that when a user eventually identifies themselves—something Cook never did—the [Session Replay Code] provider can then . . . back-reference all of that user's other web browsing." *Id.* (citation modified).

1

The six plaintiffs here who did not make purchases while using BPS's websites lack standing for the same reason as the *GameStop* plaintiff. The Session Replay Code captured the "mouse clicks and movements, keystrokes, search terms," and other actions these six plaintiffs took while browsing for products on BPS's websites. App. 99. But that information was neither sensitive nor linked to these plaintiffs' identities. So these plaintiffs "could not plausibly . . . allege that a disclosure of this information resulted in embarrassment or humiliation." *GameStop*, 148 F.4th at 159.

2

Unlike the other six plaintiffs, Cornell and Montecalvo entered their names, addresses, and payment and billing information on BPS's websites, and the Session Replay Code captured that information. Cornell and Montecalvo argue that these items of information were personal and sensitive such that their disclosure "would be highly offensive to a reasonable person." *See* Second Restatement § 652D. We agree that the "payment and billing information" was personal and sensitive, so we need not address whether the names and addresses (either independently or in combination) were as well.

When we give the allegations in the complaint "the benefit of reasonable inferences," *Lutz v. Portfolio Recovery Assocs., LLC*, 49 F.4th 323, 334 (3d Cir. 2022), "payment and billing information" refers to a complete credit card or debit card number, along with the card's expiration date and security code (hereinafter, "complete credit card or debit card number"). After all, Cornell and Montecalvo entered their "payment and billing information" to make purchases on BPS's websites, and online purchases typically require a complete credit or debit card number to finalize the transaction.

A complete credit card number grants access to a line of credit that the credit card holder must repay. And a complete debit card number allows individuals and companies to withdraw funds directly from a person's bank account. That information is highly sensitive. We have little trouble concluding that the unauthorized disclosure of a complete credit card or debit card number would cause harm analogous

to that vindicated by common-law public disclosure of private facts. *See GameStop*, 148 F.4th at 159 (rejecting the notion that Cook had shared private information, in part because Cook had not shared her "billing information while on GameStop's website"); *cf. Jones v. Bloomingdales.com, LLC*, 124 F.4th 535, 539 (8th Cir. 2024) (referring to "credit card information" as "personal information"); *Jeffries v. Volume Servs. Am., Inc*., 928 F.3d 1059, 1065–67 (D.C. Cir. 2019) (calling the printing of a full credit card number and expiration date on a receipt a "nightmare scenario" because the receipt "bore sufficient information for a criminal to defraud [the plaintiff]").

The mere collection of that sensitive information, however, is not enough to make the injury here analogous to the harm caused by the comparator tort. The comparator tort is *public disclosure* of private facts, and the harm occurs when sensitive information is *disclosed publicly*. Cornell and Montecalvo have not alleged public disclosures.

Cornell and Montecalvo allege their sensitive information was shared with the Session Replay Code Providers. But in *Barclift*, the defendant's sharing of sensitive information with a mailing vendor did not cause harm analogous to that caused by the traditional tort because Barclift's information "remain[ed] functionally internal" and was not made public. 93 F.4th at 146. The same is true here. Although the Providers store information from Cornell's and Montecalvo's visits to BPS's websites on their servers, the plaintiffs allege that the Providers do so in order to send the information back to BPS in a format that BPS can use for its business purposes. Cornell and Montecalvo do not allege that the Providers share their information with any party other than BPS. So the sensitive information BPS shares with the Providers remains functionally internal, and the injury is not analogous to that caused by a public disclosure of private facts. *See id*; *GameStop*, 148 F.4th at 159.

C

Some of these plaintiffs fare better when they analogize their alleged injuries to the harm caused by intrusion upon seclusion. Under that common-law tort, "[o]ne who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or

concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person." Restatement (Second) of Torts § 652B (1977) ("Second Restatement § 652B"); *see also GameStop*, 148 F.4th at 160.

A traditional non-physical intrusion could involve "the use of the defendant's senses, with or without mechanical aids, to oversee or overhear the plaintiff's private affairs, as by looking into his upstairs windows with binoculars or tapping his telephone wires." Second Restatement § 652B cmt. b. It could also involve other forms of unauthorized investigation or examination, like "opening [one's] private and personal mail, searching his safe or his wallet, [or] examining his private bank account." *Id.* But, unlike the public disclosure of private facts, the harm from intrusion upon seclusion "does not depend upon any publicity given to the person whose interest is invaded or to his affairs." *Id.* cmt. a. Instead, the harm arises when a defendant has "invaded a private seclusion that the plaintiff has thrown about his person or affairs." *Id.* cmt. c; *see also GameStop*, 148 F.4th at 160 (explaining that "the intrusion itself makes the defendant subject to liability," even though there is no publication or "exposure of personal or sensitive information" (citation modified)).

"The kind of harm vindicated by the intrusion-upon-seclusion tort is relatively broad." *Dickson v. Direct Energy, LP*, 69 F.4th 338, 345 (6th Cir. 2023). The breadth of the harm is apparent from the text of the Second Restatement, which addresses the interest in "solitude or seclusion [in one's] private affairs or concerns." Second Restatement § 652B; *see also id.* cmt. a (discussing the individual "interest in solitude or seclusion"); *Dickson*, 69 F.4th at 345 (recounting that the common-law tort is derived from a "generalized privacy interest"); *Lupia v. Medicredit, Inc*., 8 F.4th 1184, 1191 (10th Cir. 2021) (noting that the common-law intrusion tort "protect[s] against defendants who intrude into the private solitude of another."). The common-law tort covers a range of injuries, from those caused by persistent, hounding telephone calls to those caused by surreptitious photographs taken up one's skirt. Second Restatement § 652B cmts. c & d.

Yet this kind of harm does not have an unlimited breadth.[6] When the harm is based on an intrusion into a plaintiff's affairs, those affairs must (at least plausibly) be private. The absence of any private affairs was the fatal flaw in *GameStop*. In the complaint there, Cook "conclusorily alleged that session replay code's capability is the electronic equivalent of looking over the shoulder of each visitor to the GameStop website" and that her "electronic communications with GameStop were presumed private." 148 F.4th at 160 (citation modified). But "none of the information Cook entered on GameStop's website was personal or sensitive." *Id.* So we determined that Cook could "not plausibly allege that there was an intrusion of her solitude or seclusion as to her person or private affairs." *Id.*

1

Once again, six of the named plaintiffs (Calvert, Durham, Hernandez, Moore, Tucker, and Vonbergen) have not alleged injuries analogous to those caused by the comparator tort. These six plaintiffs could not plausibly allege that their clicks, scrolls, and searches for outdoor products on BPS's websites were private. They entered no personal or sensitive information, *see id.*, and their electronic browsing for quotidian items was no more private than the physical browsing countless shoppers do daily in BPS's brick-and-mortar stores. So the observation of those non-personal and non-sensitive interactions did not injure these plaintiffs in a manner analogous to an invasion into private affairs. *See* Second Restatement § 652B cmts. a & b; *GameStop*, 148 F.4th at 160.

The allegations about the Session Replay Code Providers' ability to aggregate information from BPS's websites to users' "fingerprints" do not help these plaintiffs

[6] Moreover, while the kind of harm vindicated by this tort is broad, liability for the tort is not. After all, liability attaches only if "the intrusion would be highly offensive to a reasonable person," and that requires a "substantial" interference with the plaintiff's seclusion. Second Restatement § 652B & cmt. d; *see also Dickson*, 69 F.4th at 345 (observing that "the *scope of liability* for the actual tort of intrusion upon seclusion is . . . circumscribed" by the highly offensive requirement).

either. According to the complaint, BPS's Providers "can" and "often [do]" aggregate data into user "fingerprints," and if the Providers link a user's identity to her "fingerprint" her other browsing history can be de-anonymized. App. 92. But that states only a theoretical path to injury, not an actual one. The plaintiffs do not allege (even upon information and belief) that the Providers used the aggregation functionality on BPS's websites. And even if they had made that allegation, it would not help the six plaintiffs who did not identify themselves on BPS's websites. Where BPS did not discover and share these plaintiffs' identities with its Providers, there are no facts upon which we could conclude that BPS helped destroy the anonymity these plaintiffs sought to maintain. So they have not alleged an injury analogous to that caused by an intrusion into their seclusion.

2

Cornell and Montecalvo, by contrast, have alleged injuries analogous to those vindicated by the intrusion-upon-seclusion tort. Unlike the other six plaintiffs, Cornell and Montecalvo entered "personal or sensitive" information when they made purchases on BPS's websites. *GameStop*, 148 F.4th at 160. Among other things, they entered their complete credit card or debit card numbers. As discussed above, that information is rightly viewed as highly sensitive. *See supra* Section II.B.2. Just as one expects her private conversations, her mail, and the contents of her wallet or bank account to be free from unwelcome "investigation or examination," Second Restatement § 652B cmt. b, one expects her complete credit card or debit card number to be free from prying eyes. So when BPS permitted its Session Replay Code Providers to surreptitiously record Cornell's and Montecalvo's complete credit card or debit card numbers, it caused those plaintiffs harm closely analogous to that vindicated by the intrusion upon seclusion tort.

The D.C. Circuit reached the same conclusion last year in a case involving comparable technology. In *Pileggi v. Washington Newspaper Publishing Company, LLC*, a news publication's website secretly embedded a computer code called "Meta Pixel" that transmitted to Meta information about the videos Pileggi watched on the website. 146 F.4th 1219,

1223, 1225 (D.C. Cir. 2025), *petition for cert. filed*, No. 25-1040 (U.S. Feb. 27, 2026). The court concluded that Pileggi's injury was analogous to that caused by an intrusion upon seclusion. It reasoned that "[a]n individual's choices about media consumption can communicate sensitive and historically private interests," so when the news publication transmitted Pileggi's video viewing history to Meta without Pileggi's knowledge or consent, it caused an intrusion that would offend a reasonable person. *Id.* at 1228; *see also Perry v. Cable News Network, Inc*., 854 F.3d 1336, 1340–41 (11th Cir. 2017) (deeming the injury from the disclosure of one's video tape rental or purchase records to be analogous to the harm caused by an intrusion upon seclusion).

Just as media consumption is sensitive and historically private, so is a person's complete credit card or debit card number. Because of how sensitive that information is, the harm resulting from its nonconsensual interception and examination closely resembles "the same interests implicated in the traditional common law cause of action of intrusion upon seclusion." *GameStop*, 148 F.4th at 160 (citation modified). Thus, Cornell and Montecalvo have standing based on their allegations that BPS embedded Session Replay Code in its websites, allowing the Providers to surreptitiously record their billing and payment information absent consent.[7]

D

The District Court correctly concluded that the six plaintiffs who made no purchases on BPS's websites lack a

[7] For some of the same reasons discussed with respect to the other six plaintiffs, neither Cornell nor Montecalvo has alleged a concrete injury arising from the Providers' ability to aggregate data from BPS's websites into "fingerprints." Cornell and Montecalvo allege only what the Session Replay Code Providers are capable of doing, not what the Providers did on BPS's websites. Absent allegations that the Providers used the aggregation functionality on BPS's websites and caused Cornell's and Montecalvo's browsing histories to be de-anonymized, there are no facts upon which we could conclude that BPS injured these plaintiffs in a manner analogous to an intrusion upon seclusion.

concrete injury to confer Article III standing, but the District Court erred in dismissing those plaintiffs' claims with prejudice. "Because the absence of standing leaves the court without subject matter jurisdiction to reach a decision on the merits, dismissals 'with prejudice' for lack of standing are generally improper." *Barclift*, 93 F.4th at 148 (citation modified). Like in *Barclift* and *GameStop*, that general rule applies here, so we will modify the District Court's order to dismiss their claims without prejudice and affirm that order as modified. *See id.*; *GameStop*, 148 F.4th at 163.

* * *

For these reasons, we will REVERSE the District Court's order as to Cornell and Montecalvo; MODIFY the District Court's order to a dismissal without prejudice as to all other plaintiffs, and AFFIRM that part of the order as modified; and REMAND for further proceedings consistent with this opinion.

Counsel for Appellant Arlie Tucker
Kate M. Baxter-Kauf **[Argued]**
Karen H. Riebel
LOCKRIDGE GRINDAL NAUEN PLLP

Counsel for Appellants Brian Calvert, Heather Cornell, Timothy Durham, Marilyn Hernandez, Greg Moore, Jr., Peter Montecalvo, Arlie Tucker, Brittany Vonbergen, and David Irvin
Carey Alexander
ARTHUR BRYANT LAW

Nicholas Colella
Jamisen A. Etzel
LYNCH CARPENTER, LLP

MaryBeth V. Gibson
THE FINLEY FIRM, PC

Steven M. Nathan
HAUSFELD

Counsel for Appellees BPS Direct LLC and Cabela's LLC
Michael E. Rayfield **[Argued]**
Jennifer A. McLoone
Maveric R. Searle
SHOOK HARDY & BACON LLP