Circuit Court for Baltimore City
Case No. 24-C-20-000591

UNREPORTED*

IN THE APPELLATE COURT

OF MARYLAND

No. 1033

September Term, 2024

JOHN DOE II

v.

MEDSTAR HEALTH, INC., *et al*.

Friedman,
Shaw,
Kehoe, Christopher
(Senior Judge, Specially Assigned)

JJ.

Opinion by Shaw, J.

Filed: March 13, 2026

*This is an unreported opinion. This opinion may not be cited as precedent within the rule of stare decisis. It may be cited for its persuasive value only if the citation conforms to Rule 1-104(a)(2)(B).

Appellant John Doe II, a MedStar Health Inc. patient, and five other individuals filed an action against Appellee, MedStar Health, Inc. and MedStar Good Samaritan Hospital, Inc. (collectively, "MedStar") asserting negligence, invasion of privacy, and a violation of the Maryland Electronic Surveillance Act ("ESA" or "Maryland Wiretap Act"), Md. Code Ann, Cts. & Jud. Proc. ("C.J.P.") § 10-401 *et seq*. in the Circuit Court for Baltimore City. They averred that Appellee knowingly and intentionally collected and shared their identifiable information and communications with Facebook and Google by "bugg[ing] its web-properties with computer code." They claimed that the collection and sharing of patient information and communications by Appellee was a violation of the confidentiality promised to patients in the MedStar "Patient Privacy Policy." Appellant and the other individuals later filed a motion requesting class certification for similarly situated MedStar patients, which was denied by the court. Appellant then filed a renewed motion.

The other individuals dismissed their claims, leaving Appellant as the sole claimant. All parties filed motions for summary judgment. At the conclusion of a hearing, the court denied Appellant's Motion for Summary Judgment and granted Appellee's Motion for Summary Judgment, awarding final judgment to Appellee on all of Appellant's claims. The court then denied Appellant's Renewed Motion for Certification as moot.

Appellant timely filed this appeal and presents three questions for our review:

1. Did the Circuit Court err in granting MedStar's Motion for Summary Judgment and denying Appellant's Motion for Summary Judgment on Appellant's claim under the ESA?

2. Did the Circuit Court err in denying Appellant's Motion for Class Certification on Appellant's claim under ESA?
3. Did the Circuit Court err in denying Appellant's Renewed Motion for Class Certification on Appellant's claim under the ESA?

For reasons that follow, we hold that the circuit court did not err in granting the motion for summary judgment. Because we hold that the Maryland Electronic Surveillance Act does not prohibit the communications that are the subject of this litigation, we decline to answers Questions 2 and 3.

BACKGROUND

Appellant, a patient of MedStar Health, is proceeding under the pseudonym, "John Doe II." From April 2018 to April 2022, Appellant logged onto the myMedStar patient portal to view certain medical information, including lab and pathology results, COVID-19 testing outcomes, radiology images, the "Health Issues" page, and "Renew Prescriptions" page. Appellant also used medstarhealth.org, the publicly available website for MedStar Health to view his doctor's biography. Appellant asserts that the contents of his communications on his myMedStar patient portal and his identifiable information, i.e. cookie values, detailed URLs, IP addresses, device attributes, user-agents, and other information, were re-directed via bugged computer code to Facebook and Google.

The complaint, at the center of this litigation, was originally filed in January 2020, in the Circuit Court for Baltimore City, by a plaintiff proceeding under the pseudonym Jane Doe against MedStar Health, Inc. and MedStar Good Samaritan Hospital, Inc. (collectively, "MedStar"). Appellant later joined. The original claim asserted that the

collection and sharing of patient information and communications by Appellee was negligent, an invasion of privacy, a breach of confidence, and a violation of both the Maryland Consumer Protection Act and the Maryland Electronic Surveillance Act ("ESA" or "Maryland Wiretap Act"), Md. Code Ann, Cts. & Jud. Proc. ("C.J.P.") § 10-401 *et seq*.

MedStar filed a Motion to Dismiss the complaint, which was denied, in part, by the court, on August 5, 2020. The court dismissed the claims regarding breach of confidentiality and breach of the Consumer Protection Act. The court declined to dismiss Jane Doe's claims of violation of the Maryland Wiretap Act, intrusion upon seclusion, and publication of private facts, stating "under these circumstances, dismissal of [these] claim[s] is inappropriate as a reasonable finder of fact could conclude that, if Plaintiff's disclosed data constitutes personally identifiable information, Defendant's disclosures are highly offensive."

An amended complaint was filed by six plaintiffs, including Appellant, on April 30, 2021. The amended complaint included four claims: a violation of the Maryland Electronic Surveillance Act ("ESA" or "Maryland Wiretap Act"), Md. Code Ann, Cts. & Jud. Proc. ("C.J.P.") § 10-401 *et seq*., two invasion of privacy claims, and negligence. On June 7, 2022, four of the six original plaintiffs, including Appellant, filed a motion for class certification. A hearing was held on November 22, 2022, and the court, on March 10, 2023, denied the Motion to Certify a Class of "[a]ll Maryland residents" who are, or were, patients of MedStar and who "exchanged communications" at MedStar's public website or patient portal before November 13, 2021. The court held that the proposed class did not

meet Maryland Rule 2-231 requirements as the class was not ascertainable; none of the plaintiffs were adequate or typical class representatives; common issues did not predominate over individualized issues for the invasion of privacy and negligence claims (two issues Appellant is not challenging on appeal); and that class certification was not the superior method of adjudication for the Maryland Wiretap Act claim.

Appellant and one other individual from the original action filed a second amended complaint on May 31, 2023. Pursuant to the Amended Scheduling Order filed by the court on June 21, 2023, the deadline for the completion of discovery was September 29, 2023.[1] On November 22, 2023, the other individual dismissed her claim with prejudice.

Appellant filed a Renewed Motion for Class Certification, which Appellee opposed. On May 15, 2024, Appellee filed a Motion for Summary Judgment based on Appellant's individual claims and Appellant filed a partial Motion for Summary Judgment. On June 26, 2024, the court granted Appellee's Motion for Summary Judgment and awarded final judgment to Appellee on all of Appellant's claims.

Appellant filed this timely appeal.

STANDARD OF REVIEW

Summary judgment is proper when "there is no genuine dispute as to any material fact and that the [moving] party is entitled to judgment as a matter of law." Maryland Rule 2-501(a). On appeal, we review the circuit court's grant of summary judgment de novo. *Gambrill v. Bd. of Educ. of Dorchester Cnty.*, 481 Md. 274, 297 (2022). "We conduct an

[1] The parties do not dispute that discovery ended on that date.

independent review of the record to determine whether a general dispute of material facts exists and whether the moving party is entitled to judgment as a matter of law." *Id*. (citation omitted).

Statutory construction most often involves an examination of the statutory text in context and a review of the legislative history to determine the statute's purpose. "To ascertain the intent of the General Assembly, we begin with the normal, plain meaning of the language of the statute." *Lockshin v. Semsker*, 412 Md. 257, 275 (2010) (citations omitted). This Court need not resort to other rules of statutory construction when the plain language of the statute unambiguously communicates the intent of the General Assembly. *Id*. (citations omitted). This Court construes the statute "'as a whole, so that no word, clause, sentence or phrase is rendered surplusage, superfluous, meaningless or nugatory.'" *Wheeling v. Selene Fin. LP*, 473 Md. 356, 376 (2013) (quoting *Koste v. Town of Oxford*, 431 Md. 14, 25–26 (2013)). This Court will neither "add nor delete language ... to reflect an intent not evidenced in the plain ... language ...." *Lockshin*, 412 Md. at 275 (citations omitted).

DISCUSSION

Motion for Summary Judgment

Appellant argues that the court erred in granting summary judgment as he successfully established each element of his Maryland Wiretap Act claim, while Appellee failed to "identify with particularity each material fact" that was in dispute, and failed to attach evidence that "demonstrates the dispute" as required by Maryland Rule 2-501(b).

Appellant asserts that the plain language and legislative history of the Maryland Wiretap Act support his claim.

Appellee argues that the data transmissions that Appellant defines as identifiable information are "not the kinds of communications the Wiretap Act was enacted to protect" and Appellant's claim was "not based on conversations between human beings, but on data transmissions between a web browser and web server relating to a user's navigation on a website." Appellee points to Section 10-401(4) and Section 10-401(10) of the Maryland Wiretap Act which states that the Act protects the interception "of the **contents** of any wire, electronic, or oral communication" and "contents" are defined as "any information concerning the identity of the parties to the communication or the existence, substance, purport, or meaning of that communication." Md. Code Ann., Cts. & Jud. Proc. §§10-401(4) – (10) (emphasis added). Because the information that Appellant is basing his claim on does not fall within the definition of "contents" under the Act, Appellee argues that the circuit court did not err.

The Maryland Wiretap Act, also known as the Electronic Surveillance Act, or "ESA", was enacted by the General Assembly in 1977 to protect private parties from improper wiretap and electronic surveillance by making it illegal to intercept or use any communication without authorization.[2] The General Assembly amended the Act in 1988 to include the interception of "electronic communications" to be consistent with Congress' enactment of the Electronic Communications Privacy Act of 1986 ("ECPA"), 18 U.S.C. §

[2] Richard P. Gilbert, *A Diagnosis, Dissection, and Prognosis of Maryland's New Wiretap and Electronic Surveillance Law*, 8 Univ. Balt. L. Rev. 183, 193-96 (1979).

2510 *et seq*. The Maryland Wiretap Act was also further amended in 1991, to broaden its jurisdiction to include mobile devices, in 1993, and in 2002, to expand device definitions and jurisdictional clarifications.

The Act is focused on the interception "of the contents of any wire, electronic, or oral communication." Md. Code Ann., Cts. & Jud. Proc. § 10-401(10). The Act defines "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system." *Id*. at 10-401(5)(i). "Contents" are defined as "any information concerning the identity of the parties to the communication or the existence, substance, purport, or meaning of that communication." *Id*. at §10-401(4). If a party is found in violation of the Act, remedies include: (1) compensatory damages, either $100 per day for each day of violation, or $1000, whichever of the two is the greater amount, (2) punitive damages, and (3) attorney fees and litigation costs.

The Act was amended after Congress passed the Electronic Communications Privacy Act and the Stored Wire Electronic Communications Act, which are commonly referred to as the Electronic Communications Privacy Act (ECPA) of 1986.[3] The ECPA updated the Federal Wiretap Act of 1968, which "addressed interception of conversations using "hard" telephone lines, but did not apply to interception of computer and other digital and electronic communications."[4] The ECPA, as amended, protects wire, oral, and

[3] *Electronic Communications Privacy Act of 1986 (ECPA)*, Office of Justice Programs: Bureau of Justice Programs, https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285 (last visited Jan. 8, 2026).
[4] *Id*.

electronic communications while those communications are being made, are in transit, and when they are stored on computers. The ECPA defines "electronic communication" as:

> **any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce**, but does not include— (A) any wire or oral communication; (B) any communication made through a tone-only paging device; (C) any communication from a tracking device (as defined in section 3117 of this title); or (D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds

18 U.S.C. § 2510(12) (emphasis added). The Act now applies to email, telephone conversations, and data stored electronically. *Id*.

The Maryland General Assembly, in creating the Maryland Wiretap Act, mirrored the language and intent of the ECPA. Accordingly, the purpose of the ECPA and the Maryland Wiretap Act are one in the same: "to protect the intrinsic subject matter of a communication and not the extrinsic fact that a communication took place. The protection is of the message, not the medium." *Sun Kin Chan v. State*, 78 Md. App. 287, 302 (1989) (citing to *United States v. New York Tel. Co.*, 434 U.S. 159, 166-67 (1977).

In *Davis v. State*, our Court examined the relationship between the Act and the Electronic Communications Privacy Act of 1986. *Davis v. State*, 199 Md. App. 273, 278 (2011). We explained that the Maryland Wiretap Act was "modeled on the federal act and closely tracks its provisions; however, the Maryland legislature has made some of the provisions of the State Act more restrictive than the federal law." *Id*. (quoting *Mustafa v.*

State, 323 Md. 65, 69 (1991)) (emphasis omitted). "[T]he two minor respects in which the Maryland law is more restrictive than its federal counterpart" are that:

> "[u]nder federal law, an interception will be lawful if either party to a conversation consents to its being overheard and recorded. In Maryland, by contrast, such an interception is lawful only if both parties give consent. *See Mustafa v. State*, 323 Md. 65 (1991). The distinction is between one-party consent and two-party consent. The closely related second distinction is that in Maryland one-party consent, as an exception to the general Maryland rule, may be enough for the investigation of certain specially designated crimes.

Davis, 199 Md. App. at 278-79. We stated, "[b]ecause the drafters of the Maryland Act so carefully tracked the federal statute ... **we look to court decisions interpreting that legislation for guidance in construing the Maryland statutory language**." *Id*. at 279 (quoting *Baldwin v. State*, 45 Md. App. 378, 380 (1980), *aff'd* 289 Md. 635 (1981)).

Central to this Court's determination of whether the court here properly granted summary judgment is an examination of whether Appellant's electronic transmissions fall within the purview of the Act. We focus on whether the statute encompasses the conduct that Appellant alleges occurred here. Because there are no Maryland cases directly addressing whether electronic transmissions and their contents fall within the purview of the Act, we look to federal caselaw interpreting the Maryland Wiretap Act's federal counterpart, the Electronic Communications Privacy Act (ECPA).

We begin with an overview of the six categories of information that Appellant claims were identifiable communication that was intercepted in violation of the Maryland Wiretap Act. Appellant alleges that "(1) cookie values; (2) IP addresses; (3) user-agents; (4) device attributes; (5) detailed URLs; and (6) other information about the substance of

the communication, such as "Login to myMedStar" were intercepted. "Cookie values" are "strings of data that a web server sends to the browser. When a browser requests an object from the same domain in the future, the browser will send the same string of data back to the origin server."[5] An "IP address" is the abbreviation for Internet Protocol address, which is "a unique number which identifies a computer and its location on the Internet; a logical address assigned to every workstation, server, printer, and router on a connected network."[6] "User-agent" is the term used to describe "software—typically a web browser, bot, or application—acting on behalf of a user to interact with web servers. It sends an HTTP header string identifying the browser, version, and operating system to the server, allowing websites to tailor content for the user's device."[7] "Device attributes" refers to a:

> characteristic or property associated with a particular device. It typically describes specific features, capabilities, or configurations that define the functionality or behavior of the device. Device attributes can include physical parameters (such as size, weight, or color), technical specifications (such as processing power, storage capacity, or connectivity options), or software settings (such as display brightness, notification preferences, or security

[5] Stephen Fiebrandt, *What are cookies? What are the differences between them (session vs. persistent)?,* Cisco, https://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/117925-technote-csc-00.html (last updated Jan. 27, 2026).

[6] *IP address,* Oxford Reference, https://www.oxfordreference.com/display/10.1093/oi/authority.20110803100010535#:~:text='IP%20address'%20can%20also%20refer,IP%20address'%20in%20Oxford%20Reference%20%C2%BB (last visited Jan. 27, 2026).

[7] *User Agent,* Mozilla Developer Network Glossary (2025), https://developer.mozilla.org/en-US/docs/Glossary/User_agent (last visited Jan. 27, 2026).

> settings). They provide essential information to users, developers, or system administrators to understand and interact with the device effectively.[8]

"URLs", which is the abbreviation for Uniform Resource Location, are used to navigate the Internet from website to website, as well as through various webpages on a singular website.[9] Appellant adds the qualifier "detailed," stating that the URL contained more information than simply the website or webpage name. Appellant asserts that "other information about the substance of the communication, such as 'Login to myMedStar'" is a category of information that was intercepted in violation of the ESA. We view this as a catchall category.

The Ninth Circuit, examined, in the case of *In re Zynga Privacy Litigation*, 750 F.3d 1098, 1106 (9th Cir. 2014), the word "contents" as used in the Electronic Communications Privacy Act of 1986 ("ECPA"). There, a class of Facebook users sued Facebook and Zynga Game Network, Inc., a third-party game app that Facebook users can access without leaving their Facebook page. *Id*. at 1100. To play Zynga games, a Facebook user is required to click on a link for the game; the link then sends an electronic request to Zynga for access to the game. *Id*. at 1102. In order to clarify "what happens when a

[8] *Device Attribute*, Ontology of Personal Information (OPI) Project, https://opi.cs.cmu.edu/show/device_attribute (last visited Jan. 27, 2026).

[9] TECH TIPS: WHAT IS A URL? (2023), https://www.oppl.org/news-events/digital-learning/tech-tips-what-is-a-url/#:~:text=Every%20website%20has%20a%20unique%20address%20called,you%20want%20to%20visit%20on%20the%20web (last visited Jan 27, 2026).

Facebook user clicks on a link or icon," prior to its analysis, the Court provided a "brief review of how computers communicate on the internet":

> The hypertext transfer protocol, or HTTP, is the language of data transfer on the internet and facilitates the exchange of information between computers. R. Fielding, et al., Hypertext Transfer Protocol—HTTP/1.1, § 1.1 (1999), http://www.w3.org/Protocols/HTTP/1.1/rfc2616.pdf. The protocol governs how communications occur between "clients" and "servers." A "client" is often a software application, such as a web browser, that sends requests to connect with a server. A server responds to the requests by, for instance, providing a "resource," which is the requested information or content. *Id*. §§ 1.3, 1.4. Uniform Resource Locators, or URLs, both identify a resource and describe its location or address. *Id*. §§ 3.2, 3.2.2. And so when users enter URL addresses into their web browser using the "http" web address format, or click on hyperlinks, they are actually telling their web browsers (the client) which resources to request and where to find them. *Id*. § 3.2.2.
>
> The "basic unit of HTTP communication" is the message, which can be either a request from a client to a server or a response from a server to a client. *Id.* §§ 1.3, 4.1. A request message has several components, including a request line, the resource identified by the request, and request header fields. *Id*. § 5. The request line specifies the action to be performed on the identified resource. *Id*. § 5.1. Often, the request line includes "GET," which means "retrieve whatever information ... is identified by the" indicated resource, or "POST," which requests that the server accept a body of information enclosed in the request, such as an email message. *Id*. §§ 9.3, 9.5. For example, if a web user clicked a link on the Ninth Circuit website to access recently published opinions (URL: http://www.ca9.uscourts. gov/opinions/), the client request line would state "GET/opinions/HTTP/1.1," which is the resource, followed by "Host:www.ca9.uscourts.gov," a location header that specifies the website that hosts the resource. *Id*. § 5.1.2.
>
> Other request headers follow the request line and "allow the client to pass additional information about the request, and about the client itself, to the server." *Id*. § 5.3. **A request header known as the "referer" provides the address of the webpage from which the request was sent.** *Id*. § 14.36. For example, if a web user accessed the Ninth Circuit's website from the Northern District of California's webpage, the GET request would include the following header: "Referer: http://www.cand.uscourts.gov/home."

In re Zynga Priv. Litig., 750 F.3d at 1101-02 (emphasis added).

The Court explained that when a Facebook user clicked on a link to play a Zynga game, the link generated a request that included "referer-header" information that indicated which user was sending the request and what page the user was viewing. *Id*. at 1102. Zynga then provided access to the requested game based on information provided in the referer-header request. *Id*. During this process, Zynga collected the user's identity and page location from the referer header information. That information was then sold to advertisers and other third parties.

The class of users argued that Zynga had disclosed their personal information without their consent, in violation of the federal Electronic Communications Privacy Act (ECPA). *Id*. at 1103. They argued that the webpage addresses contained in the referer headers, "revealed the contents of a communication, because they disclose specific information regarding a webpage that a user previously viewed." *Id.* at 1108.

The Ninth Circuit did not agree. The Court held that the referer header information, which contained the Plaintiffs' user IDs and visited webpage addresses, included "only basic identification and address information, not a search term or similar communication made by the user." *Id*. at 1109. As a result, the Court held that it did not "constitute the contents of a communication." *Id*. at 1108-09. The court, further, stated that, "**Congress intended the word 'contents' to mean a person's intended message to another** (i.e. the 'essential part' of the communication, the 'meaning conveyed', and the 'thing one intends to convey')." *Id*. at 1106 (emphasis added). The court emphasized that the term "'contents' does not include 'record' information", which is information that contains the "'name',

'address', and 'subscriber number or identity' of a subscriber or customer." *Id*. The court concluded that "[t]here is no language in ECPA equating 'contents' with personally identifiable information. Thus, an allegation that Facebook and Zynga disclosed personally identifiable information is not equivalent to an allegation that they disclosed the contents of a communication." *Id*. at 1107. Because the information within the referer headers at issue in *Zynga* only contained "record" information at most, the court held that the appellees did not violate the ECPA. *Id*. at 1109.

Here, while Appellant does not allege that Appellee used "referer headers", the categories of information that Appellant *does* allege Appellee used that were intercepted, concern the same type of activity and "record information" that the Ninth Circuit held does not constitute "contents" under the ECPA. As defined above, cookie values, IP addresses, device attributes, user-agents, and URLs (the categories of information Appellant alleges were intercepted) all operate similarly to referer headers; they are automatic functions that computers or electronic devices connected to the Internet use as part of the HTTP request-response cycle. A device sends a string of metadata, which is data about data, such as cookie values, an IP address, a URL, and attributes of the device, to the server the device is attempting to gain access to (the request), the server receives the metadata, and then permits the device access to the content that the device user was attempting to view (response). This activity, and record information passed during the HTTP request-response cycle, similar to the referer header requests in *Zynga*, "does not meet the definition of

'contents,' because these pieces of information are not the 'substance, purport, or meaning' of a communication." *In re Zynga Priv. Litig.*, 750 F.3d 1098, 1107 (9th Cir. 2014).

In a case brought in the Third Circuit, *In re Google Inc.*, the definition of "contents" was also examined. There, "internet users brought actions against internet advertising providers, alleging that providers placed tracing cookies on users' browsers in contravention of browsers' cookie blockers" and asserted, among other claims, violations of the federal Wiretap Act. *In re Google Inc.*, 806 F.3d 125, 137 (3d Cir. 2015). The Court found that the term "contents" does not include "dialing, routing, addressing, or signaling" information, such as "addresses, phone numbers, and URLs . . . when they are performing such a function." *In re Google Inc.*, 806 F.3d at 137. The Third Circuit affirmed, in part and vacated in part, finding, that the users had adequately pled that providers collected "content" under the Wiretap Act. The Court cited *Smith v. Maryland*, where the Supreme Court explained "the important difference between extrinsic information used to route a communication and the communicated content itself." *Id*. at 135; *see generally Smith v. Maryland*, 442 U.S. 741 (1979) (holding that pen registers "disclose only the telephone numbers that have been dialed – a means of establishing communication. Neither the purport of any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed is disclosed by pen registers."). The Third Circuit emphasized that, pursuant to *Smith*, other courts have held that "[l]ocation identifiers have classically been associated with non-content 'means of establishing communication.'" *Id*. at 136. Location identifiers serve "no routing function but instead

comprises part of a communication's substance . . . In essence, addresses, phone numbers, and URLs may be dialing, routing, addressing, or signaling information, but only when they are performing such a function. If an address, phone number, or URL is instead part of the **substantive information conveyed to the recipient,** then by definition, it is 'content.'" *In re Google Inc.*, 806 F.3d at 136-37 (emphasis added).

Another case, *Cook v. GameStop Inc.*, 689 F.Supp.3d 58 (W.D. Pa. 2023), elaborated on how URLs may or may not be defined as "contents" under the ECPA. As discussed prior, URLs (Uniform Resource Location) are used to navigate the Internet from website to website, as well as through various webpages on a singular website. In *Cook*, a website user, Amber Cook, brought a putative class action suit against online retailer, GameStop, Inc., asserting claims for "violation of Pennsylvania Wiretapping and Electronic Surveillance Control Act and tort of intrusion upon seclusion" based on GameStop's use of a program that recorded, saved, and replayed visitors' interactions with its online website. *Cook*, 689 F.Supp. 3d at 58. The Pennsylvania Wiretapping and Electronic Surveillance Control Act is "patterned after its federal counterpart, the Electronic Communications Privacy Act" and "prohibits the interception of an electronic communication without prior consent." *Id*. at 68. Cook argued that GameStop captured a record of the URLs of webpages she visited while on GameStop's website, a violation of the Pennsylvania Wiretap Act. *Id*. at 70. The U.S. District Court for the Western District of Pennsylvania found that "[n]avigating through a website's multiple pages is *not the substance of a communication*; it's an action taken to go to a digital location." *Id*. at 70

(emphasis added). The court stated, that "in the final calculus, 'whether a URL involves "contents" depends "on how much information would be revealed by disclosure of the URL.'" *Id*. at 71 (citing *In re Google*, 806 F.3d at 138 (2015)).

In *Rodriguez v. FastMed Urgent Care, P.C.*, 741 F.Supp.3d 352 (2024), a case similar in facts to the instant case, the plaintiff, Jackelyn Rodriguez, a FastMed[10] patient, used "FastMed's [] website and MyChart portal to schedule appointments, locate FastMed providers and locations, find information on specific health conditions, treatments, and medications, message doctors, view doctors notes, schedule appointments, and review medications." *Rodriguez*, 741 F. Supp.3d at 358. Rodriguez brought claims against FastMed similar to those brought by Appellant here. She alleged that FastMed shared her individually-identifiable health information with Meta for commercial gain without her consent and thereby violated HIPAA, federal regulations, state regulations, and FastMed's privacy policies." *Id*. She brought the action on behalf of herself and others similarly situated. *Id*. She filed the action, claiming, "(1) a violation of the Electronic Communications Privacy Act, Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510 et seq., (2) negligence under North Carolina law, (3) invasion of privacy for intrusion upon seclusion under North Carolina law, and (4) a violation of the North Carolina Electronic Surveillance Act." *Id*. at 357. Rodriguez alleged that "FastMed worked with Meta 'to design Meta Pixels that intercept the characteristics and content of

[10] FastMed is an integrated healthcare provider/payer system in Raleigh, North Carolina, operating nearly 200 medical clinics in Arizona, Florida, North Carolina, and Texas.

electronic communications containing individually-identifiable health information' to 'transmit this information to Meta.'" *Id*. at 363.

The plaintiff's claim under the federal Wiretap Act was dismissed without prejudice. The court found that "Rodriguez has not plausibly alleged that FastMed, not Meta, intercepted her information in violation of the statute" and "[b]ecause FastMed was a party to Rodriguez's communication and FastMed 'intercepted' Rodriguez's individually-identifiable health information with her prior consent, FastMed did not violate 18 U.S.C. §2520(a) [the ECPA]." *Id.*

In the case at bar, Appellant did not assert, nor was there any evidence in the record, that showed that a communication between him and another person was transmitted to Google or Facebook. He navigated to the myMedStar patient portal login page.

During the hearing on the Motion for Summary Judgment, the court asked counsel for Appellant:

> THE COURT: . . . What gets sent to Google and Facebook?"
>
> MR. BARNES: A log in. The fact that they are logging in the literally the status of the log in . . .
>
> THE COURT: . . . I want to make clear that there is no allegation or proof that the email address or the password is being sent to Google or Facebook.
>
> MR. BARNES: That's right, but it's not necessary.
>
> THE COURT: I'm not asking that question. . . I want to exactly understand because you said login communications. I wanted to understand what you meant by that.
>
> [. . .]

> MR. BARNES: Email address and password not sent to Google. Here is what is sent, the login, the fact of a login - -
>
> THE COURT: Okay.[11]

According to counsel for Appellant, Appellant's email address and password to his myMedStar patient portal login are not sent to Google or Facebook; rather, the fact that there was a login is sent to Google and Facebook.

We find persuasive the Ninth Circuit's finding that "[n]avigating through a website's multiple pages is **not** the substance of a communication; it's an action taken to go to a digital location." *Cook*, 689 F.Supp.3d at 70 (emphasis added).

As to Appellant's contention regarding URLs, we note that counsel for Appellee ("Ms. Scully") explained to the court that the URLs that Appellant alleges provided personal information were not protected content under the Maryland Wiretap Act:

> MS. SCULLY: Here, for the URL string that that I showed you that's at issue for the lab results, you cannot determine any particular lab result that John Doe looked at. There is - - that's just a generic name of a tab. It does not reflect the particular document that was reviewed. It does not reflect any search that John Doe made. And so that is why those cases are distinguishable from the cases - - from the situation and the facts here, and why John Doe doesn't have a viable cause of action, wiretap cause of action, on the content piece of it.[12]

Appellee's counsel referenced *Brown v. Google LLC*, 685 F. Supp. 3d 909 (N.D. Cal. 2023). In that case, the "detailed URL" at issue was a URL associated with a Google search "for updates on Russia's war against Ukraine on the Washington Post's 'World' section."

[11] Record Extract – Part I of XI, Exhibit 212 – 213.
[12] Record Extract – Part I of XI, Exhibit 257.

Brown, 685 F. Supp. 3d at 936. The URL was held to be "content" under the ECPA because it included "the particular document within a website that a person view[ed] [and] divulg[ed] a user's personal interests, queries, and habits." *Id*. at 935-36.

The URLs at issue in the present case do *not* reference a particular document or lab result; rather, the URLs state the generic name of the tab that Appellant was visiting. The URLs reflect Appellant's *activity*, namely his visiting the myMedStar patient portal login page and publicly accessing the MedStar webpage. The only possible "detailed URL" at issue is that which showed Appellant's navigation within the myMedStar patient portal to the "myMedStar Lab Results" tab. We note, however, "[t]here is no evidence that [Doe] ever clicked [the 'Login to myMedstar' button]," as stated in the June 26, 2024 Motions Hearing:

> THE COURT: Where's the evidence that John Doe II clicked that button?
>
> MR. BARNES: John Doe II said that hedid [sic] log in. He the evidence is that he enrolled. Okay. There is no direct evidence of the date and time that he clicked this button.
>
> THE COURT: There is no evidence that he ever clicked it.
>
> MR. BARNES: I don't – I think the he would say he did not recall, so that's that's [sic] fair enough.[13]

As for the "IP addresses" and "cookie values" that Appellant alleges were leaked, the IP address that was transmitted from Appellee's public website and the myMedStar patient portal login page to Google and Facebook, were anonymized IP addresses and "that is

[13] Record Extract – Part I of XI, Exhibit 284.

undisputed."[14] "An IP address, even if not anonymized, doesn't concern someone's identity. An IP address concerns the access point to the internet."[15] Similarly, cookie values also do not identify a person – "they identify a browser and a device," and the cookie values used by Google in this case are anonymized.[16] Applying the holdings of both *In re Zynga* and *In re Google Inc.*, we hold that the "record information" that cookie values transmit are not "contents" under the ECPA, and by association the Maryland Wiretap Act. The cookie value data is "not sufficient to show that the data that was transmitted was information that relates to the identity of the person,"[17] and therefore, Appellee's use of them is not a violation of either statute.

In sum, the circuit court did not err in granting the motion for summary judgment. The Maryland Wiretap Act does not prohibit or protect the collection and sharing of Appellant's electronic communications while navigating the myMedStar patient portal or MedStar's publicly available website. The sharing of "detailed URLs", IP addresses, cookie values, and "the fact of a login" to Google and Facebook, are not defined as "contents" under the Act.

JUDGMENT OF THE CIRCUIT COURT FOR BALTIMORE CITY AFFIRMED; COSTS TO BE PAID BY APPELLANT.

[14] *Id*. at Exhibit 257.
[15] *Id*.
[16] *Id*. at Exhibit 258.
[17] *Id.*