

RECEIVED

Sep 17 2026

SC Court of Appeals

**THE STATE OF SOUTH CAROLINA
In the Court of Appeals**

**APPEAL FROM CHARLESTON COUNTY
Court of Common Pleas**

Civil Action Court Case No. 2025-CP-10-04577

Appellate Case No. _____

The Bastion Group, LLC and Aaron Willard,

Petitioners,

v.

Robbins Construction Group, LLC

Respondent.

**MEMORANDUM IN SUPPORT OF PETITIONERS' MOTION TO SUPPRESS
EVIDENCE PURSUANT TO S.C. CODE ANN. § 17-30-110**

I. INTRODUCTION

Petitioners, Aaron Willard ("Willard") and The Bastion Group LLC ("Bastion") move to suppress all electronic communications, text messages, and derivative evidence and pleadings obtained by Respondent Robbins Construction Group, LLC, ("Robbins") through unauthorized real-time interception of Willard's smartphone communications. The electronic communications accessed on Willard's smartphones included both personal and business communications. Bastion's confidential business information and legal advice from its attorneys were contained in Willard's business communications on his smartphones. Robbins reactivated a Windows Phone Link connection on an old Dell laptop previously used by Willard and used that connection to acquire Willard's text messages from his

Samsung S22 and S25 smartphones in real time. This conduct constitutes an unlawful interception of electronic communications under S.C. Code Ann. § 17-30-20. The intercepted communications and all evidence derived therefrom must be suppressed under S.C. Code Ann. § 17-30-110.

II. STATEMENT OF FACTS

Willard was formerly employed by Robbins During that employment; Willard used a Dell laptop owned by Robbins. After Willard's employment ended, Robbins obtained access to that laptop. Robbins then reactivated a Windows Phone Link connection from the laptop to Willard's personal Samsung S22 and S25 smartphones. Through this connection, Robbins obtained Willard's text messages in real time as they were being transmitted. Willard noticed a series of connections from Robbins' Dell laptop to his phones over the course of a year from July 2025 to July 2026. The final proof of this interception occurred on June 9, 2026, when Robbins attached a text message, intercepted from Willard's S25 smartphone on June 8, 2026, on an email sent to a client that both Robbins and Willard's new company, Bastion, were competing for. The nature and full scope of the communications obtained by Robbins will be established at the evidentiary hearing.

Microsoft Phone Link software paired with the built-in Link to Windows software on the Samsung S25 smartphone automatically forwards all incoming/outgoing SMS messages to the paired PC creating a perfect "interception" scenario.

Microsoft describes Phone Link/Link to Windows as a continuing connection between the Android phone and PC. Once message permission is enabled messages from the Android device are synced to and displayed on the PC without any action by the phone user. (See

<https://insights.samsung.com/2024/08/23/how-to-use-link-to-windows-on-your-galaxy-smartphone-5/>).

Once Microsoft Phone Link was secretly reactivated and connected on Willard's S25 smartphone, whenever new SMS messages arrived, Link to Windows automatically acquired/synchronized the contents and made them available on the Dell PC in Robbins' possession in real-time as the messages were being received on the phone. This closely linked mechanism provides a substantial argument that the acquisition of Willard's electronic communications was an "interception", rather than merely unauthorized access to stored communications. The acquisition mechanism in the paired Phone Link and Link to Windows functions prospectively: each newly arriving communication is automatically captured by the linked system without the phone owner having to open the message or the bad actor needing to later retrieve it manually. A nearly perfect mechanism when misused to provide continuous interceptions of SMS traffic on the Samsung phone.

This Phone Link and Link to Windows is Microsoft's answer to Apple's sharing iMessage traffic across multiple Apple devices. This Court has already ordered that unauthorized use of Apple's iMessage sharing across devices could constitute an interception per the SCHSA when a bad actor uses a connected device to spy on the text message traffic of a non-consenting victim. (See *Justin Shayne Fulmer, Respondent, v. Melissa Emery Buckhannon Esq., et al, Anna Coggeshall, Petitioner*. Appellate Case No. 2022-000330).

III. LEGAL STANDARD

Under S.C. Code Ann. § 17-30-110, "A person who intentionally intercepts, attempts to intercept, or procures another person to intercept or attempt to intercept any wire, oral, or

electronic communication is guilty of a felony." The South Carolina Homeland Security Act (SCHSA) governs the interception of electronic communications and is patterned after the federal Electronic Communications Privacy Act of 1986 (ECPA). Because the SCHSA mirrors the ECPA, South Carolina courts import federal judicial interpretation and construe the two statutes identically. *18 USCS § 2518*, *UNITED STATES v. GIORDANO*, 416 U.S. 505, 530 (1974). S.C. Code Ann. § 17-30-20 defines "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." *18 USCS § 2510*. To constitute a qualifying intercept, the acquisition of the electronic communication must occur contemporaneously with its transmission by its sender. *Luis v. Zang*, 833 F.3d 619, 627 (2016), *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 878 (2002), *United States v. Steiger*, 318 F.3d 1039, 1047 (2003). A qualifying intercept occurs when the electronic communication is accessed at some point between the time the communication is sent and the time it is received by the destination server. *Global Policy Partners, LLC v. Yessin*, 686 F. Supp. 2d 631, 638 (2009). Once a communication is delivered and stored, it is considered a stored communication rather than an active interception. *Luis v. Zang*, 833 F.3d 619, 627 (2016), *Columbia Pictures, Inc. v. Bunnell*, 245 F.R.D. 443, 450 (2007). When evidence has been obtained in violation of the SCHSA, S.C. Code Ann. § 17-30-110 provides for suppression. Under the parallel federal statute, *18 U.S.C. § 2518(10)(a)*, an aggrieved person may move to suppress the contents of any intercepted communication or evidence derived therefrom on the grounds that the communication was unlawfully intercepted, the order of authorization was insufficient on its face, or the interception was not made in conformity with the order of authorization. *18 USCS § 2518*. Whenever any electronic communication has been

intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence if the disclosure of that information would be in violation of the statutory scheme. *18 USCS § 2515*. This exclusionary mandate extends to all derivative evidence obtained as a result of the original unlawful interception. *UNITED STATES v. GIORDANO*, 416 U.S. 505, 530 (1974), *United States v. Spagnuolo*, 549 F.2d 705, 712 (1977).

IV. ARGUMENT

A. Robbins' Real-Time Access to Willard's Text Messages Constitutes an Unlawful Interception Under S.C. Code Ann. § 17-30-20 Robbins's acquisition of Willard's text messages satisfies the statutory definition of an unlawful interception. An "intercept" is the acquisition of the contents of any electronic communication through the use of any electronic, mechanical, or other device. *18 USCS § 2510*. Text messages transmitted via smartphone constitute electronic communications within the meaning of the statute. *Id.* An electronic communication is defined 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. *Id.* The critical element is contemporaneity. Courts applying the ECPA have consistently held that a qualifying intercept occurs only where the acquisition of the communication occurs contemporaneously with its transmission by its sender. *Global Policy Partners, LLC v. Yessin*, 686 F. Supp. 2d 631, 638 (2009). Interception includes accessing messages in transient storage on a server during the course of transmission, but does not include accessing the messages stored on a destination server. *Id.* The term intercept applies solely to the transfer of electronic signals and does not apply to the acquisition of electronic

signals that are no longer being transferred. *Luis v. Zang*, 833 F.3d 619, 627 (2016).

Interception must catch the communication in flight before the communication comes to rest and ceases to be a communication. *Id.* Robbins obtained Willard's text messages in real time. This real-time acquisition satisfies the contemporaneous transmission standard required for an interception. *18 USCS § 2518*, *UNITED STATES v. GIORDANO*, 416 U.S. 505, 530 (1974). The Windows Phone Link connection enabled Robbins to acquire communications as they were being transmitted, not after they had been received and stored on the destination device. This distinction is dispositive. Accessing a stored communication does not constitute an intercept within the meaning of the statute. *Global Policy Partners, LLC v. Yessin*, 686 F. Supp. 2d 631, 638 (2009). But acquiring a communication during its transmission—catching it in flight—does. *Luis v. Zang*, 833 F.3d 619, 627 (2016), *United States v. Steiger*, 318 F.3d 1039, 1047 (2003). Robbins used the laptop as an electronic device to acquire the contents of Willard's electronic communications through the Phone Link connection. This conduct falls squarely within the statutory definition of interception. *18 USCS § 2510*.

B. Robbins's Interception Was Unlawful Because It Was Conducted Without Authorization or Consent Under S.C. Code Ann. § 17-30-30(C), an interception is lawful only if the person intercepting the communication is a party to the communication, or if one of the parties to the communication has given prior consent to the interception. Robbins was not a party to any of the communications between Willard and third parties. Willard did not give prior consent to the real-time monitoring of his personal smartphone communications. The absence of consent is established in Willard's attached affidavit. Even if Robbins initially had authorization to access company-owned devices during Willard's employment, such authorization terminated upon the end of the employment relationship. Absent explicit,

prior consent from Willard or another party to the specific real-time communications being intercepted, Robbins's real-time monitoring does not fall under any statutory exception and constitutes an unlawful interception.

C. All Evidence Derived from the Unlawful Interception Must Be Suppressed.

The exclusionary mandate of S.C. Code Ann. § 17-30-110 and its federal counterpart, 18 U.S.C. § 2515, requires suppression of both the primary intercepted communications and all derivative evidence. Whenever any electronic communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any proceeding if the disclosure of that information would be in violation of the statutory scheme. *18 USCS § 2515*. The suppression extends to all derivative evidence—communications or information obtained as a result of the original unlawful interception—even if obtained under a subsequent judicial order, provided that the subsequent evidence was based on or intertwined with unlawfully obtained evidence. Because the interception here was unlawful, all evidence that flows from it is subject to the exclusionary rule. *UNITED STATES v. GIORDANO*, 416 U.S. 505, 530 (1974), *18 USCS § 2515*.

D. The Scope of Accessible Electronic Communications Through Windows Phone Link Reinforces the Seriousness of the Statutory Violation. Through a smartphone connection such as Windows Phone Link, an individual can extract or access virtually any data stored on or transmitted through the device, including call logs, contacts, photos, applications (including sensitive application data from banking and healthcare applications), emails, voicemails, social media items, and web pages. The real-time nature of the connection means that Robbins had the technical capability to intercept not only text messages but also any other electronic communication transmitted to or from Willard's

smartphones. While the specific scope of what Robbins actually obtained will be established at the evidentiary hearing, the technical capability of the connection demonstrates the invasive nature of the interception and the breadth of Willard's privacy interest at stake. The statute protects against precisely this kind of unauthorized real-time surveillance of electronic communications. *18 USCS § 2510, 18 USCS § 2515.*

E. Not Every Statutory Defect Requires Suppression, But Unlawful Interception Does. Suppression of evidence is not required for every failure to satisfy a statutory requirement in Title III or its state-law counterpart. Suppression is warranted only for violations of provisions that directly and substantially implement Congress's intention to restrict use of intercept procedures to the circumstances clearly requiring such measures. *United States v. Dahda*, 853 F.3d 1101, 1111 (2017). Not all deficiencies in wiretap applications warrant suppression. *Id.* However, the statutory grounds for suppression include unlawful interception itself. *18 USCS § 2518, United States v. Staffeldt*, 451 F.3d 578, 580 (2006). Section 2518(10)(a) provides for suppression when the communication was unlawfully intercepted, the order of authorization or approval under which it was intercepted is insufficient on its face, or the interception was not made in conformity with the order of authorization or approval. *18 USCS § 2518, Id.* These are the exclusive grounds for suppression under Title III. *United States v. Jackson*, 849 F.3d 540, 551 (2017). Here, the violation is not a technical defect in an otherwise lawful wiretap application. Robbins conducted a warrantless, unconsented, real-time interception of Willard's electronic communications. This is an unlawful interception under subsection (i) of § 2518(10)(a) and its state-law equivalent. *Id.* The Supreme Court has held that subsection (i) includes constitutional violations and outlaws official interceptions without probable cause. *Id.*

Suppression is therefore mandatory. *18 USCS § 2515, United States v. Scurry*, 821 F.3d 1, 7 (2016).

V. CONCLUSION

Robbins's real-time acquisition of Willard's text messages through the reactivated Windows Phone Link connection constitutes an unlawful interception of electronic communications under S.C. Code Ann. § 17-30-20. The acquisition occurred contemporaneously with transmission, satisfying the statutory definition of interception. Robbins was not a party to the communications, and Willard did not consent. Any prior authorization for Robbins to monitor Willard's electronic communications terminated with his employment. The intercepted communications and all evidence derived therefrom are subject to the exclusionary mandate of S.C. Code Ann. § 17-30-110 and must be suppressed.

VI. PRAYER FOR RELIEF

WHEREFORE, Petitioners respectfully request that this Court:

1. Grant Petitioners' Motion to Suppress and suppress all electronic communications, text messages, and other data obtained by Robbins through the unlawful interception of Willard's smartphone communications;
2. Suppress all evidence derived from the unlawfully intercepted communications, including any statements, physical evidence, or investigative leads obtained as a result of the interception;
3. Conduct an evidentiary hearing to determine the full scope of the interception, the duration of the monitoring, and the extent to which the unlawfully obtained evidence informed the investigation and the civil suit brought by Respondent against Petitioners; and
4. Grant such other and further relief as the Court deems just and proper.

Respectfully submitted,

/s Steven M. Abrams
Steven M. Abrams, Esquire
Abrams Cyber Law & Forensics, LLC
SC Bar No. 76230
1154 Holly Bend Drive
Mount Pleasant, SC 29466
843.813.1996
steve@abramscyberlaw.com
Attorney for Petitioners

September 17, 2026