April 21, 2025

Senator Anthony Broadman
Member, Oregon Senate Committee on the Judiciary
900 Court St. NE, S-423
Salem, Oregon 97301
Email: Sen.AnthonyBroadman@oregonlegislature.gov

Subject: Concerns Regarding HB 3865A

Dear Senator Broadman,

My name is Chiara McPhee, and I serve as the Chief Product Officer for Postscript, a leading platform in the e-commerce ecosystem that empowers businesses to build direct relationships with their customers through SMS and other messaging channels. In this capacity, I am responsible for the overarching product vision and execution at Postscript, ensuring our offerings not only drive value for the thousands of merchants we support but also operate within the bounds of an increasingly intricate regulatory environment surrounding mobile communications. This necessitates a deep understanding of both the technical underpinnings of the text messaging ecosystem and the evolving legal landscape that governs it.

Before joining Postscript, my career has been deeply entrenched in the evolution of the mobile messaging ecosystem. For over a decade, I worked in various capacities within companies that provided infrastructure and services enabling mobile communication. This included early work in the mobile network space, where I gained firsthand experience with the intricacies of network signaling and subscriber data management. I subsequently spent several years at a mobile marketing technology provider, where I led efforts to build compliant and effective communication strategies for businesses leveraging SMS and other emerging messaging channels. This journey provided me with a comprehensive understanding of the technical capabilities and limitations of the messaging ecosystem, the crucial importance of respecting consumer preferences, and the increasing focus from regulatory bodies, particularly the Federal Communications Commission (FCC), on consumer privacy within this domain. My experience has underscored the delicate balance that businesses must strike between effective communication and diligent adherence to evolving regulations.

Beyond my professional endeavors in the technology sector, I am also a proud and engaged resident of Bend, Oregon. I attended Oregon Episcopal School in Portland, and after obtaining my undergrad at Duke and MBA from Standard, I returned to Oregon so I could raise my family in this vibrant community that I'm proud to call home. I am invested in the well-being of our state and its businesses. The innovative spirit and strong sense of community here in Oregon are values I deeply cherish, and it is with this perspective – as

both a technology leader in the messaging space and an Oregonian – that I am writing to you today to express significant concerns regarding House Bill 3865A.

I. Compliance with HB3865A's Restrictions is Practically Impossible Given the Federal and State Focus on Securing Location-Based Data

A key aspect of understanding the challenges posed by HB 3865 relates to the historical, and now largely unavailable, methods for inferring the geographic location of mobile subscribers. One such technical mechanism that businesses previously might have considered, albeit with recognized limitations in accuracy and completeness, was the use of Home Location Register (HLR) Lookups.

HLR Lookups involve the real-time querying of a mobile network's Home Location Register, which is a central database containing essential information about each mobile subscriber authorized to use that network. Historically, by querying the HLR, it was possible to retrieve details from the mobile carrier about a subscriber's "home" network affiliation, and queries could return a subscriber's current geographic location based on the visited mobile switching center (VMSC). While this process did not provide real-time GPS-level location tracking, it could be an effective proxy for a subscriber's general geographic location sufficient to understand the associated time zone for a device before a message was transmitted.

However, the feasibility and legality of utilizing such tools for location determination have been fundamentally altered by a significant and imminently reasonable shift at the federal and state level towards prioritizing the privacy of consumer communications data. Chiefly, the FCC, in its interpretation and enforcement of Section 222 of the Communications Act (47 U.S.C. § 222), has adopted an increasingly stringent stance on the confidentiality of Customer Proprietary Network Information (CPNI). Crucially, the FCC has made it clear that location information falls squarely within the definition of CPNI and is therefore subject to robust privacy protections.[1]

Over the past several years, the FCC has consistently emphasized that mobile carriers bear a direct and non-delegable responsibility to protect their customers' CPNI, which includes data revealing their location. This stance was reinforced by notable enforcement actions taken against the major mobile carriers concerning the unauthorized disclosure of customer location data through Location Based Services (LBS) programs. In 2024, following a multi-year investigation, T-Mobile was ordered to pay $80 million, along with a $12 million fine for its subsidiary, Sprint, which it had acquired in 2020. AT&T was fined and ordered to pay more than $57 million and Verizon was fined almost $7 million, underscoring the FCC's firm belief that even indirect methods of accessing or sharing

---

[1] *In Re: AT&T, Inc.*, Forfeiture Order, 39 FCC Rcd. 4216 (Apr. 29, 2024), *vacated by AT&T, Inc. v. FCC*, 2025 U.S. App. LEXIS 9172 (5th Cir., Apr. 17, 2025); *In re: T-Mobile USA, Inc.*, 39 FCC Rcd. 4350 (Apr. 29, 2024); *In re: Sprint Corp.*, 39 FCC Rcd. 4305 (Apr. 29, 2024).

location data without explicit and verifiable consumer consent were in violation of Section 222 and the associated CPNI rules. The FCC's concern was that location data shared with third parties without the carrier obtaining a clear and affirmative opt-in from the consumer, posed significant privacy risks.

The direct consequence of these FCC decisions and the associated heightened has made it impossible for SMS platforms like Postscript to use HLR Lookups for the purpose of geographic location determination. As the FCC's position on the impermissible sharing of location data without explicit consent became increasingly firm and the potential for substantial penalties for CPNI violations grew, mobile carriers became extremely cautious about providing detailed location-related information to third-party entities through HLR Lookups. The legal and financial risks associated with potentially violating Section 222 far outweighed any perceived benefits of providing this type of data to third-party services seeking to infer geographic location.

This evolution towards stronger consumer privacy safeguards has been a progressive process, also reflected in the increasing focus at the state level on securing consumer's location-based data.[2] Consequently, location-based information necessary to gain a general understanding of a mobile subscriber's geographic area, has been significantly restricted, to the point of being unusable for this purpose by law-abiding companies. This means not only cannot Postscript not know where a message will be delivered in the United States before it is sent, none of the 18,000 small and mid-size businesses across the country who rely on Postscript to communicate with their customers can either.

The ramifications of this fundamental shift are particularly pertinent to proposed state-level legislation such as HB 3865A, which would put both Postscript and its customers at risk for class action litigation by imposing specific regulations on mobile messaging within Oregon, including establishing "Quiet Hours" that may differ from

---

[2] *See, e.g.,* Oregon Department of Justice, *Google: AG Rosenblum Announces Largest AG Consumer Privacy Settlement in U.S. History* (Nov. 14, 2022), *available at:* https://www.doj.state.or.us/media-home/news-media-releases/largest-ag-consumer-privacy-settlement-in-u-s-history/ ("location data is among the most sensitive and valuable personal information Google collects. Even a limited amount of location data can expose a person's identity and routines and can be used to infer personal details."); State of California Department of Justice, *Attorney General Bonta Announces Investigative Sweep of Location Data Industry, Compliance with California Consumer Privacy Act* (March 10, 2025), *available at:* https://oag.ca.gov/news/press-releases/attorney-general-bonta-announces-investigative-sweep-location-data-industry ("Because location data could be weaponized to locate individuals offline, businesses should be keenly aware of their responsibilities to protect this data and ensure consumers understand their rights."); California Privacy Protection Agency, State Regulators Form Bipartisan Consortium to Collaborate on Privacy Issues (Apr. 16, 2025), *available at:* https://cppa.ca.gov/announcements/2025/20250416.html (announcing that California, Oregon, and six other states have formed a pact to investigate potential privacy law violations, including issues surrounding location data).

federal guidelines or common industry practices. This inability to obtain reliable real-time location data is a direct outcome of the federal government's commitment to safe-guarding consumer privacy, a commitment that I know Oregon shares. However, this essential prioritization of individual privacy has a tangible and significant consequence: it effectively eliminates the very tools that businesses might have previously employed to attempt to adhere to geographically specific regulations like those contemplated in HB 3865A.

II. Businesses Who Obtain Prior Consent Should Not Be Subjected to Conflicting Legal Obligations

The lack of ability to obtain location-based data is particularly important with regard to HB 3865A, which differs materially from federal law and the laws in other states with regard to its treatment of businesses who obtain prior consent. As Chief Product Officer for Postscript, I have the good fortune of spending considerable time talking with ecommerce companies across the country about their businesses and their concerns. Therefore, I understand firsthand the complexities businesses face in navigating the evolving landscape of mobile messaging regulations. For small and mid-size businesses (SMBs), in particular, the need for uniformity at both the state and federal level is essential. Notably, other states that have adopted state-specific laws concerning quiet hours for text messaging did so before the FCC finalized its enforcement action against the wireless carriers in 2024.[3]

It is critical to appreciate that ecommerce businesses invest significant resources in marketing and building trust with consumers so that consumers feel comfortable signing up for their SMS list – that is, providing their prior consent to receive SMS messages from the brand. Indeed, I am very proud that Postscript, as a leader in compliance, only works with ecommerce brands that obtain prior express written consent – the highest level of consent under federal law.

The imposition of disparate state-specific regulations, such as the proposed "quiet hours" in HB 3865A starting at 7 PM Pacific even with prior consent, creates an untenable situation for SMBs that often operate across state lines. Unlike larger corporations with dedicated legal and compliance teams, SMBs typically have fewer resources to track and adhere to a patchwork of potentially conflicting requirements. The technical impossibility of accurately determining the real-time location of mobile subscribers further exacerbates this challenge, leaving SMBs vulnerable to inadvertent violations and costly legal challenges simply for communicating with customers who have explicitly requested to receive their messages. This regulatory fragmentation not only increases operational burdens and diverts limited resources from crucial areas like innovation and customer service but also creates a chilling effect, potentially discouraging SMBs from leveraging SMS and other messaging channels to engage with their customer base effectively. A consistent and predictable regulatory framework is essential to empower SMBs to build

[3] Connecticut (2023); Florida (2021); Maryland (2023); Oklahoma (2022); Virginia (2020); Washington (2022).

direct relationships with their customers confidently and to foster a fair and competitive marketplace.

Furthermore, the principle of prior express written consent should serve as a cornerstone of any mobile messaging regulation. When a consumer willingly provides their explicit agreement to receive communications, they have indicated their desire to engage with that business. Deviating from federal standards that recognize this consent, as seen in HB 3865A's proposed restrictions even for consented messages, opens the door to a surge in frivolous litigation targeting legitimate businesses. Plaintiff firms are increasingly exploiting ambiguities in state laws, leading to costly settlements and a misdirection of legal focus away from truly harmful unsolicited communications. For SMBs, the financial and operational burden of defending against such lawsuits can be particularly devastating. Uniform protections grounded in the principle that prior express written consent negates the need for state-specific "quiet hours" or other restrictions would provide the clarity and predictability SMBs need to operate without the constant threat of opportunistic litigation.

III. Oregon Law Should Not Impede the Adoption of RCS, Which Has the Power to Curb Fraud

Finally, I want to share with you my views about why HB3865A should not regulate Rich Communication Services (RCS) in the manner that is currently proposed. Postscript is at the forefront of testing RCS for businesses in the United States and I see immense potential in RCS to revolutionize how businesses connect with their customers while simultaneously bolstering trust and security in mobile messaging. Unlike traditional SMS and MMS, RCS offers a far more interactive and transparent experience, allowing for branded messaging with logos, rich media like images and videos, interactive buttons, and carousels. This enhanced engagement can significantly improve marketing campaigns, customer support interactions, and overall brand communication.

Crucially, RCS is designed with robust security features at its core. Its tightly controlled ecosystem, which includes stringent verification processes for businesses and the display of brand logos within messages, makes it significantly harder for malicious actors to impersonate legitimate companies and perpetrate fraud or phishing attempts. Google's requirement for trusted partners to manage sender agents on behalf of brands, with permissions needed from both the brand and mobile operators, adds another critical layer of authentication. This inherent focus on verification and branding provides a much safer environment for consumers, enabling them to confidently engage with businesses they recognize and trust, a stark contrast to the vulnerabilities often exploited in SMS.

Given RCS's powerful capabilities in both enhancing business-to-consumer communication and mitigating fraud, the prospect of unnecessary state-based regulations, such as those proposed in HB 3865A, is deeply concerning. The FCC has rightly recognized RCS as distinct from traditional SMS and MMS, clarifying that it is not subject to federal telemarketing regulations. Oregon's attempt to impose state-specific rules on RCS, treating it as identical to these older protocols, not only disregards its

fundamental technological differences but also creates a significant barrier to its widespread adoption. As with the "quiet hours" and message limitation proposals for SMS, the impracticality of determining a user's real-time location makes compliance with state-specific RCS regulations virtually impossible for businesses operating across state lines. This regulatory uncertainty and the potential for unintentional violations will undoubtedly cause a chilling effect, discouraging businesses, especially SMBs with limited resources, from investing in and deploying RCS.

The irony here is that HB 3865, in its aim to curb messaging-based fraud, could inadvertently prolong it by hindering the adoption of a technology specifically designed with superior anti-fraud mechanisms. By creating a fragmented and burdensome regulatory landscape for RCS, Oregon risks delaying the very transition to a more secure messaging environment that would better protect its citizens. A national, consistent framework that acknowledges the unique attributes and security benefits of RCS is essential to foster its growth and allow businesses to leverage its full potential in combating fraud. Imposing premature and ill-fitting state regulations will only stifle innovation and delay the deployment of a messaging technology that holds significant promise for a safer and more effective communication landscape for both businesses and consumers.

Thank you for your time, attention, and thoughtful consideration of these critical issues. As a resident of Bend and a leader in the mobile messaging ecosystem, I am deeply concerned about the potential unintended consequences of HB 3865 in the current regulatory environment and would welcome the opportunity to discuss these concerns and explore potential solutions further.

Sincerely,

Chiara McPhee

Chiara McPhee
Chief Product Officer, Postscript
Resident of Bend, Oregon

Cc: Senator Floyd Prozanski, Chair (Sen.FloydProzanski@OregonLegislature.gov)
Senator Kim Thatcher, Vice Chair (Sen.KimThatcher@oregonlegislature.gov)
Senator Sara Gelser Blouin (Sen.SaraGelser@oregonlegislature.gov)
Senator James I. Manning, Jr. (Sen.JamesManning@oregonlegislature.gov)
Senator Mike McLane (Sen.MikeMcLane@oregonlegislature.gov)