



April 21, 2025

The Hon. Floyd Prozanski
Chair, Senate Committee on Judiciary
Sen.FloydProzanski@OregonLegislature.gov

The Hon. Kim Thatcher
Vice Chair, Senate Committee on Judiciary
Sen.KimThatcher@oregonlegislature.gov

The Hon. Anthony Broadman
Member, Senate Committee on Judiciary
Sen.AnthonyBroadman@oregonlegislature.gov

The Hon. Sara Gelser Blouin
Member, Senate Committee on Judiciary
Sen.SaraGelser@oregonlegislature.gov

The Hon. James I. Manning, Jr.
Member, Senate Committee on Judiciary
Sen.JamesManning@oregonlegislature.gov

The Hon. Mike McLane
Member, Senate Committee on Judiciary
Sen.MikeMcLane@oregonlegislature.gov

Subject: Concerns Regarding House Bill 3865A and its Potential Impact on the Global Mobile Messaging Ecosystem

Dear Members of the Senate Committee on Judiciary,

The Mobile Ecosystem Forum (MEF) writes to you today to express our significant concerns regarding Oregon House Bill 3865A, as amended, and its potential ramifications for businesses operating within the United States and globally that utilize mobile messaging to connect with consumers. MEF is a global trade association comprised of companies whose products power a wide range of mobile services, including messaging, content, advertising, and the Internet of Things (IoT). Our membership spans across 45 countries and includes mobile network operators, OS and platform providers, device manufacturers, media and content owners, app developers, brands and agencies, financial institutions, privacy and security specialists, technology providers, billing providers, mobile marketing firms, and professional services.

MEF provides a platform for our members to collaborate, share best practices, and influence the industry agenda through various initiatives, including working groups, regulatory consultations, and the development of industry codes of conduct. We have a uniquely international view of the mobile ecosystem and are committed to fostering a healthy and innovative environment for mobile communications.

MEF has been at the forefront of working to find technical solutions to prevent SMS spam and fraud for years. Since 2016, MEF members have worked on a Business SMS Fraud Framework to develop best practice guidelines for the Business messaging industry. Further, SMS Sender ID Protection Registries run by MEF in the UK, Ireland & Spain have had considerable impact on combating SMS Phishing & Spoofing. MEF's RCS Working Group, established in January 2023, focuses on how global wireless carriers are using RCS A2P messaging (also known as Rich Business Messaging or RBM) to provide a "more secure" business messaging channel by leveraging verified sender ID requirements within the RCS framework.



We have been made aware of the advancements of House Bill 3865A, which seeks to regulate telephone solicitations within Oregon. While we understand and appreciate the intent behind this legislation to protect consumers from unwanted communications, we are concerned that the members of the House Committee on Commerce and Consumer Protection and its Chair, Representative Sosa, have not adequately considered the practical consequences of the proposed legislation. We have identified several provisions that pose significant technical challenges for businesses and could inadvertently hinder legitimate and desired interactions, potentially creating unintended negative consequences that extend beyond the state of Oregon.

One of our primary concerns stems from the bill's proposed regulation of Rich Communication Services (RCS). HB 3865 would expressly regulate RCS, a modern messaging protocol that offers enhanced features compared to SMS and MMS. To our knowledge, this would represent the first state law to specifically regulate RCS. It is crucial to note that the Federal Communications Commission (FCC) has made it clear that RCS is not subject to the federal Telephone Consumer Protection Act (TCPA). Introducing state-specific regulations for a technology that operates across networks and national borders creates a complex and potentially conflicting regulatory landscape for businesses to navigate.

RBM is an efficient tool to mitigate SMS Spoofing and SMS Phishing, for two key reasons:

- Authorised developers/aggregators/MNOs: only authorised developers or aggregators (i.e., those who have a contract with an MNO or are a Google RBM partner) and MNOs can send RBM traffic.
- Brand verification: RBM has strict brand verification rules, which forces the identity of the sender behind each RCS bot/agent to be known and brand verified.

RCS delivers greater security by offering end-to-end encryption and verified business profiles. That is, RCS uses technology that supports a tunneled or encrypted connection to carriers and was designed to require verification of a sender's cryptographic credentials before their name and logo are displayed to users, therefore it is much more difficult to impersonate an RCS sender. Furthermore, the vetting and verification process is much stricter than SMS and MMS messaging channels, making it virtually impossible for fraudsters to impersonate a business. Consider, for example, if each message sent to a consumer from their bank was delivered from the bank's verified business profile. This would help customers instantly distinguish legitimate communications from potential scams. That's the world that MEF and its members are building. For example, MEF's RCS working group anticipates that approximately 90% of the fraud currently derived from SMS Spoofing, and 70% of fraud deriving from SMS Phishing, could be blocked via RBM using RCS APIs.

A critical technical challenge of imposing regulation on RCS technology at the state level arises from the fact that it is practically impossible for a business to definitively know when it is sending an RCS message to a recipient physically located within Oregon at any given moment. Mobile phone users travel frequently, and privacy protections prevent businesses from accessing real-time location-based data from wireless carriers. Imposing regulations that hinge on the recipient's real-time location, without the ability to reliably determine that location, places an unreasonable burden on businesses and creates a significant risk of



unintentional non-compliance. This could lead to unwarranted legal exposure, particularly for companies operating on a national or global scale.

Furthermore, we are concerned about the "quiet hours" provision in HB 3865A, which reportedly proposes to start at 7 PM Pacific in Oregon, even for consumers who have provided prior express written consent to receive messages. This deviates from the federal standard of 8 a.m. to 9 p.m., which generally applies to calls and text messages sent without prior express consent. The discrepancy between state and federal "quiet hours" regulations exacerbates the technical difficulties associated with location determination. As highlighted in petitions to the FCC by the Ecommerce Innovation Alliance (EIA) and other businesses, the inability to access real-time location data for wireless phones makes compliance with location-based "quiet hours" provisions exceedingly difficult. This has already led to a rise in what many consider to be frivolous lawsuits based on time zone discrepancies. Oregon's adoption of a different "quiet hours" standard would further complicate compliance for businesses operating nationwide, potentially interfering with the creation of a more uniform national standard. Even with prior express written consent, which the FCC has acknowledged as a valid basis for communication, the proposed Oregon bill appears to impose restrictions based on location, a factor that is technically impossible to ascertain before a business transmits a message.

We also understand that HB 3865A may require companies to include specific disclosures in text messages, drawing from ORS 646.611(1). While transparency is important, imposing disclosure requirements that may not be relevant to the context of text message marketing adds unnecessary complexity. Moreover, the difficulty in determining when a mobile phone is within Oregon's borders makes it practically challenging for national businesses to dynamically alter message content to comply with state-specific disclosure mandates. The national standard generally focuses on brand identification within the message, and adding further layers of location-dependent disclosures creates operational hurdles.

The cumulative effect of these technically challenging provisions could have a chilling effect on the adoption of innovative messaging technologies like RCS by businesses. The increased risk of non-compliance and potential litigation may deter companies from leveraging these enhanced communication methods, ultimately hindering the evolution of mobile messaging and potentially disadvantaging Oregon consumers who could benefit from richer and more interactive messaging experiences.

For businesses operating across state lines and internationally, consistency in regulatory frameworks is paramount. Divergent state-specific regulations, particularly those that are technically difficult to comply with, create significant operational burdens and costs. This can stifle innovation, increase compliance overhead, and potentially lead businesses to limit their engagement with consumers in states with particularly complex or technically challenging requirements.

We urge the members of the Senate Committee on Labor and Business to carefully consider the technical limitations inherent in regulating mobile communications based on real-time location and the potential negative impact that HB 3865A, in its current form, could have on businesses both within the US and beyond. We believe that a more harmonized approach,



aligned with federal regulations where they exist and cognizant of the global nature of mobile messaging, would better serve both consumers and businesses.

MEF and our members are committed to working constructively with policymakers to ensure a safe, effective, and innovative mobile ecosystem. We would welcome the opportunity to discuss these concerns further with the Committee and offer our expertise on the technical and regulatory landscape of the global mobile messaging ecosystem.

Thank you for your time and consideration of these important issues.

Sincerely,

Dario Betti,

CEO, Mobile Ecosystem Forum (MEF)

Dario@mobileecosystemforum.com

+44 7989 6875 07

<https://mobileecosystemforum.com/>