Seattle Journal of Technology, Environmental & Innovation Law

Volume 13 | Issue 1 Article 7

2023

# From Spying to Mindreading: Expanding wiretapping legislation to protect customers' privacy of thought from chat preview in online chat functions

John Deming
jdeming@seattleu.edu

# From Spying to Mindreading: Expanding wiretapping legislation to protect customers' privacy of thought from chat preview in online chat functions

John Deming

## I. INTRODUCTION

In this day and age, mass collection of customer data by businesses is an everyday reality. This practice makes customers' personal information readily available over the Internet, including some content that may be otherwise unavailable through public records[1] and presumptively private in nature. It can almost seem at times as if exposing intimate personal information to companies like Google or Facebook has become as commonplace and mundane as sharing one's credit history with a bank or giving an insurance company access to medical records.

Yet, contemporary online data harvesting differs from these disclosures of information, not only in scale, but also in kind. On the Internet, businesses can obtain everything from fairly trivial personal details to deeply private information, such as a customer's location,[2] facial features,[3] or even personal genetic information.[4] Naturally, some of these interactions are likely to elicit discomfort from ordinary Internet users, either because of the specific information involved or the surreptitiousness with which it is extracted. The present article will address this second concern and discuss a subset of these furtive data procurements.

To begin, consider the following personal anecdote: several years ago, I worked at a customer service call center for a company that offered independent study courses to high school and college students. Like many businesses, our company had a chat feature on its website to connect customers with customer service representatives. During a casual work conversation, one of my colleagues began to explain how the chat function worked. He showed me what the interface looked like, how he logged in, how the chat team organized and divided work, etc. He then told me something that I have been thinking about ever since: before a customer hit "send" on a message, he could see what the customer was typing or erasing as it happened.

My colleague then discussed how useful this feature was in helping him assist customers and how he occasionally laughed at some of the

[1] Alexander Tsesis, *The Right to Erasure: Privacy, Data Brokers, and the Indefinite Retention of Data*, 49 WAKE FOREST L. REV. 433, 442 (2014).
[2] *See* Lisa A. Schmidt, *Social Networking and the Fourth Amendment: Location Tracking on Facebook, Twitter, and Foursquare*, 22 CORNELL J.L. & PUB. POL'Y 515 517-18 (2012).
[3] See Blake A. Klinkner, *Facial Recognition Technology, Biometric Identifiers, and Standing to Litigate Invasions of Digital Privacy*, WYO. LAW., October 2019, at 44.
[4] *See* Kristi Harbord, *Genetic Data Privacy Solutions in the Gdpr*, 7 TEX. A&M L. REV. 269, 270 (2019).

angry things that customers would type but not send. I left this conversation thinking two things: (1) that if a tiny company like ours had access to such technology it must surely be available to other businesses as well, and (2) that if I were a customer, I would be deeply uncomfortable with having my messages previewed in this manner, especially without my knowledge or consent.

This article posits that chat preview is an invasion of consumers' privacy of thought and seeks to advocate for customers by proposing limitations on businesses' ability to preview their customers' unsent messages. Specifically, it argues that a party to an online chat who wishes to monitor another party's as yet unsent messages should be legally required to (1) notify and obtain the other party's consent before beginning to monitor and (2) cease monitoring at the request of the other party at any time. It will discuss the privacy implications of technology that enables customer service agents to see what customers type in real time, prior to the customer using the "send" button or analogous feature to formally send a message. Section II of this article provides a brief overview of this technology, which I shall call 'chat preview,' including how it works and what its uses are. Section III analogizes chat preview to wiretapping and analyzes federal and state wiretapping statutes. This analysis will include a summary of the relevant portions of the Electronic Communications Privacy Act (ECPA) at the federal level and the Washington State wiretapping statute at the state level. Section IV evaluates the extent to which previewing a customer's chat messages implicates each statute and discusses pertinent policy concerns. More particularly, this section discusses the fundamentality of the right to be free from intrusion on private, unexpressed thoughts, as well as the necessity of robust protections to guard that right from intrusive chat preview. Finally, Section V, details how the specific proposal of conversation-by-conversation disclosure and consent will serve consumers better than the current wiretap statute regime and provide the necessary protections to customer privacy. This section will also address potential counterarguments and concerns about the practicality of the proposed changes.

## II. BACKGROUND

While some customers may be surprised to learn that chat preview technology exists at all, what may be even more surprising is how ubiquitous it is. Companies like IKEA, PayPal[5], and McDonalds[6] all use this function when chatting with customers online. Far from being a niche curiosity, this technology is advertised by multiple chat software

[5] *Real-time typing view,* LIVE AGENT (last visited Apr. 14, 2022), https://www.liveagent.com/features/real-time-typing-view [https://perma.cc/TS4G-NHRJ].

[6] Press Release, Annie Palmer, Be careful what you write! Customer service agents can see what you're typing BEFORE you press send in live chats (Nov. 28, 2018), https://www.dailymail.co.uk/sciencetech/article-6439485/Be-careful-write-Customer-service-agents-youre-typing-press-send.html [https://perma.cc/4GRZ-4QUZ].

companies as a major selling point of their products.[7] LiveChat, one of several chat software companies whose product includes a chat preview function, provides software to over 33,000 companies,[8] while WhosOn boasts over 10,000 customers, including over 10% of Fortune 500 brands.[9] Despite its widespread use, the actual feature that enables agents to see messages before they are sent does not have a standard name in the industry; rather, it is called various things, such as "message sneak peek," "real-time typing view," and "chat preview," depending on the company.[10] For the sake of clarity and consistency, this article will use the term "chat preview" throughout.

As a preliminary matter, it seems practical to provide a working definition of what this article means by "chat preview." For the purpose of this analysis, chat preview will be defined as (1) an asymmetric feature in an online interaction or communication (2) which allows one party, but not the other, to (3) view the typed matter of another party as it is typed and before the typing party pushes a "send" button or engages some analogous function to send what they have typed. This article focuses primarily on the context of online chats between customers and customer service agents, but chat preview may also foreseeably occur in a other settings as well.

That businesses may embrace chat preview is understandable, as it can certainly be useful for customer service agents. For one thing, previewing customers' messages allows agents to respond more quickly, and thereby prevents businesses from losing customers due to long wait times for service.[11] Faster service times could also logically reduce long queues and thus reduce employee stress. Chat preview providers also advertise benefits such as anticipating and detecting the mood and attitude of each individual customer, facilitating multi-tasking, and ferreting out abusive customer interactions more quickly.[12]

These chat preview functions are made possible by Javascript, a coding language used in most websites[13] that detects what a user is doing

---

[7] *See Chat preview,* WHOSON (last visited Apr. 14, 2022), https://www.whoson.com/features/chat-preview [https://perma.cc/5BAH-DSE3]; *Real-time typing view, supra* note 5; Alicja Pawliczak, *Chat section overview,* LIVEAGENT (last visited Apr. 14, 2022), https://www.livechat.com/help/how-to-chat-window [https://perma.cc/P6MB-ZLHA].

[8] *36,000+ companies choose LiveChat to connect with customers*, LIVECHAT (last visited Apr. 14, 2022), https://www.livechat.com/customers [https://perma.cc/2Y9L-R6L4].

[9] *Customers*, WHOSON (last visited Apr. 15, 2022), https://www.whoson.com/customers [https://perma.cc/3QVB-WAGS].

[10] *See Chat preview, supra* note 7; *Real-time typing view, supra* note 5; Pawliczak, *supra* note 7.

[11] *See Real-time typing view, supra* note 5 (indicating that one in five customers reports willingness to stop patronizing businesses because of slow service).

[12] *See Chat preview*, supra note 7.

[13] Lisa Vaas, *Are the websites you're using tracking what you type?*, Naked Security (Dec.17, 2013), https://nakedsecurity.sophos.com/2013/12/17/are-the-websites-youre-using-tracking-what-you-type [https://perma.cc/X3MY-MZMA].

on the website as it happens.[14] This tracking capability includes information such as mouse clicks, the position of the user's cursor, and keystrokes made on the user's keyboard.[15] While this seems invasive, and indeed can be leveraged to perform intrusive tasks, this is not necessarily some new, Orwellian innovation. In fact, as Lisa Vaas explains, much of the basic functionality of the Internet would be impossible without Javascript: "[The tracking capabilities of Javascript] aren't intrinsically bad things. In fact [,] they're enormously useful. Without those sort of capabilities [,] sites like Facebook and Gmail would be almost unusable, searches wouldn't auto-suggest and Google Docs wouldn't save our bacon in the background."[16] Indeed, even without the intervention of a chat software, almost anyone who owns and operates a website can still track the inputs of users in real time.[17]

Yet, the technological mundanity of this tracking capability does not necessarily mean that every application of it is benign or free of privacy concerns. For example, this same technology allows companies like Quicken Loans to collect and store data from forms that customers begin to fill out, even if they ultimately decide not to submit the form[18] precisely to avoid giving up their data. Chat preview enables a similar type of interception and recording. Chat preview concerns written matter that, like the unsubmitted Quicken Loans forms, is still uncompleted and unsent, thereby exposing not only what the customer has said, but also what they are *about to* say or, in more severe cases, what they have decided at the last minute *not* to say. In other words, it exposes the user's thoughts to an audience with whom they have not yet chosen to share them.

## III. FEDERAL AND STATE WIRETAPPING STATUTES

As demonstrated above, chat preview is not terribly dissimilar from wiretapping, a practice that also deprives a speaker of their right to choose the audience for their communication, and that conjures images of all sorts of invasions on individual privacy. The principal difference between chat preview and wiretapping is that a wiretap expands the audience of a communication without the communicator's consent, whereas chat preview creates an audience where the communicator has not yet decided to allow any audience at all. If anything, this implies that chat preview poses a greater threat to privacy than a traditional wiretap. At least in the case of wiretapping, the speaker has chosen to share their thoughts with someone, even if that person is not the one on the end of the wiretap.

However, as we proceed to use wiretapping legislation as a framework to understand the current state of the law as it applies to chat preview functions, it is important to note this important difference from the outset. The comparison between wiretapping and chat preview is an admittedly

---

[14] Kashmir Hill, *Be Warned: Customer Service Agents Can See What You're Typing in Real Time*, GIZMODO (Nov. 27, 2018), https://gizmodo.com/be-warned-customer-service-agents-can-see-what-youre-t-1830688119 [https://perma.cc/2KHS-L9CJ].
[15] Vaas, *supra* note 15.
[16] *Id.*
[17] *Id.*
[18] Hill, *supra* note 18.

imperfect one. It may be precisely for this reason that, as we will discuss later, the statutes that currently exist to combat wiretapping are ill-equipped to protect users from chat-preview-based intrusions on the privacy of their unsent messages.

*A. Federal Law: The Electronic Communications Privacy Act (ECPA)*

The relevant portion of 18 U.S.C. § 2511—also known as the Electronic Communications Privacy Act (ECPA) or the Wiretap Act[19]—makes it a federal crime to intercept electronic communications.[20] Under the act, wiretapping victims can also bring a civil action against those who have intercepted their communications.[21] The statute covers not only successful interceptions, but also "any person who . . . endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication . . ."[22]

The ECPA defines "intercept" to mean "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."[23] The "device" language precludes interception claims based on mere unaided perception.[24] This language also places limits on which acquisitions constitute interceptions. For example, a person who acquires metadata indicating that a text message has been sent to a specific number has not "intercepted" the message. [25]

Under the ECPA, the interception element also requires that the contents of the communications be acquired contemporaneous to their transmission.[26] For example, in *Pure Power Boot Camp v. Warrior Fitness Boot Camp*, an employer fired an employee and subsequently accessed and printed out the former employee's e-mails from personal e-mail accounts that were saved on a company computer.[27] The e-mails included messages that the ex-employee had drafted and sent from his home computer and even some messages dated after his termination.[28] The district court, citing cases decided in other federal jurisdictions, found that the interception element under the ECPA was not satisfied because, rather

[19] *In re Carrier IQ, Inc.*, 78 F. Supp. 3d 1051 1076 (N.D. Cal. 2015).
[20] Interception and disclosure of wire, oral, or electronic communications prohibited,18 U.S.C.A. § 2511(1)(a) (1948).
[21] Recovery of civil damages authorized, 18 U.S.C.A. § 2520 (1948).
[22] 18 U.S.C.A. § 2511(1) (1948).
[23] Definitions, 18 U.S.C.A. § 2510(4) (1948).
[24] *See* Aldrich v. Ruano, 952 F. Supp. 2d 295 302 (D. Mass. 2013), *aff'd*, 554 F. App'x 28 (1st Cir. 2014).
[25] *See* In re Carrier IQ, Inc., 78 F. Supp. 3d 1051 (N.D. Cal. 2015) (holding that plaintiffs failed to state a claim against a company whose software made simultaneous records of phone numbers to which plaintiffs sent text messages).
[26] *See Pure Power Boot Camp v. Warrior Fitness Boot Camp*, 587 F. Supp. 2d 548, 557 (S.D.N.Y. 2008).
[27] *Id*. at 552.
[28] *Id*. at 553.

than obtaining the messages in the process of their delivery, the employer accessed e-mails that had already been delivered.[29] The defendants in the case, while conceding the existence of the contemporaneousness requirement, argued that a message can still be contemporaneously intercepted if it is captured shortly after its transmission and within a certain amount of time. [30] However, the district court rejected this argument, finding it lacking in specificity, evidentiary support, and supporting authority.[31]

In addition to the contemporaneousness requirement, the ECPA further limits protections against wiretapping. The act explicitly exempts "provider[s] of wire or electronic communication service[s]" from criminal and civil liability for intercepting electronic communications "in the normal course of [their] employment while engaged in any activity which is a necessary incident to the rendition of [their] service."[32] Furthermore, the definition of the type of instruments by which an interception can take place explicitly excludes devices provided to a user or subscriber and used by the subscriber in their ordinary course of business.[33] In *Hall v. EarthLink Network*,[34] the plaintiff alleged that EarthLink violated the ECPA by continuing to receive and store e-mails sent to his EarthLink e-mail address after terminating his account access for allegedly sending spam.[35] The appellate court found that EarthLink did not violate the ECPA because all available evidence indicated that EarthLink acted "within the ordinary course of business," and therefore its actions did not meet the statutory definition of interception, and therefore did not violate the act.[36]

Additionally, the ECPA defines "electronic communication" more narrowly than the plain language meaning of the term may suggest. Section 2510(12) restricts the definition of electronic communications to those communications that are "transmitted in whole or in part by… system[s] that [affect] interstate or foreign commerce."[37] This may, at first blush, appear to be nothing more than a jurisdictional safeguard, but it carries with it important implications. One implication of this requirement is that, in many cases, it may exclude data collected from a computer if that data has not been sent anywhere beyond the computer itself.[38] This definition means that the act protects people from having their message go to the wrong place once out of their hands but does not protect them from having it taken from them before they send it. For example, in *United States v. Ropp*, the defendant was indicted for installing a device on an office computer that captured and recorded keystrokes as they were transmitted from the computer's keyboard to its CPU.[39] The district court

[29] *Id*. at 556-58.
[30] *Id*. at 557.
[31] *Id*.
[32] 18 U.S.C.A. § 2511(2)(a)(i) (1948).
[33] 18 U.S.C.A. § 2510(5)(a) (1948).
[34] *See Hall v. EarthLink Network, Inc*., 396 F.3d 500 (2d Cir. 2005).
[35] *Id*. at 502.
[36] EarthLink, 396 F.3d at 503-05; *see also* 18 U.S.C.A. § 2510(5)(a).
[37] 18 U.S.C.A. § 2510(12).
[38] *See e.g. United States v. Ropp*, 347 F. Supp. 2d 831 (C.D. Cal. 2004).
[39] *Id*. at 831.

explained that the defendant did not violate the ECPA because, while the computer had connectivity to a system that affected interstate commerce, the intercepted data was not transmitted by that system.[40] The court in *Rene v. G.F. Fishers* reached a similar conclusion.[41] In that case, the plaintiff's bosses allowed her to access her personal checking and e-mail accounts without her knowing that a keylogging software was installed on her work computer.[42] The defendants then used the plaintiff's retrieved keystrokes to obtain her passwords to those accounts.[43] The court found that the keystrokes, while obtained "in transit," were not electronic communications under the act because, at the time of their seizure, the keystrokes were transmitted internally on the plaintiff's computer instead of externally to a system that affected interstate commerce.[44]

*Rene* also signals that the interception and electronic communication elements of the offense under the ECPA are interrelated.[45] The district court explained that the nature of the system employed by the keylogger negated not only the electronic communication element but also the interception element, stating that "[b]ecause the intercepted keystrokes were not electronic communications, they could not be "intercepted" as that term is defined in the [ECPA]."[46] The Court of Appeals for the Eleventh Circuit has similarly declared that "use of a keylogger will not violate the Wiretap Act if the signal or information captured from the keystrokes is not at that time being transmitted beyond the computer on which the keylogger is installed (or being otherwise transmitted by a system that affects interstate commerce)."[47] The reasoning for this is simple: if the act criminalizes the interception of electronic communications and the material that a defendant has captured is not an electronic communication, then the capture is not an illegal interception. The practical implication of this intersection, at least according to these courts, seems to be that in a case where one person seizes electronic signals or data from another, it may involve an electronic communication without an interception, but it cannot involve an interception without an electronic communication.[48]

Another relevant provision of the act provides that, so long as a communication is not intercepted for the purpose of committing some other unlawful act, interceptions of electronic or other protected

---

[40] *Id*. at 837-38.
[41] *See Rene v. G.F. Fishers*, Inc., 817 F. Supp. 2d 1090 (S.D. Ind. 2011).
[42] *Id*. at 1092.
[43] *Id*.
[44] *Id*. at 1094.
[45] *See id.*
[46] *Id*.
[47] *United States v. Barrington*, 648 F.3d 1178, 1202 (11th Cir. 2011).
[48] *But see In re Carrier IQ, Inc.*, 78 F. Supp. 3d 1051, 1079, 1076-82 (N.D. Cal. 2015) (holding that plaintiffs' complaint properly alleged an interception despite defendants' argument that acquired data was not an electronic communication because it was acquired while still on plaintiffs' phones).

communications by parties to the communication are not unlawful.[49] This appears to mean that mere invasion of another's privacy via wiretapping may be insufficient to establish liability. Likewise, if any party to the communication gives prior consent to an interception of the communication, the interception does not violate the ECPA.[50]

### *B. State Law: Washington State's Anti-Wiretapping Statute*

In addition to the protections provided in federal law, state laws may provide consumers additional protection from unwanted data interception. Here we will focus on Washington's anti-wiretapping statute, which is a state statute analogous to the ECPA.

While the two acts are different in several meaningful ways, there is also significant overlap between them. Most notably, an interception of an electronic communication, as defined in the ECPA, without the consent of any party to the communication is likely to violate the Washington statute as well in many instances.[51] Additionally, just like the ECPA, the Washington law establishes both criminal[52] and civil[53] liability for unlawful interceptions. The two laws also resemble one another in that they each contain a provision generally prohibiting evidence obtained by an unlawful interception under the respective act from being admitted in court.[54]

However, the two acts take decidedly different approaches to regulating seizures of communications. For one thing, the Washington statute, as a state and not a federal law, does not adopt the ECPA's narrow, interstate-commerce-dependent definition of "electronic communications."[55] Also, the ECPA generally puts a comparatively greater emphasis on cataloging and categorizing protected communications by type—wire communications, oral communications, and electronic communications.[56] By contrast, the Washington statute emphasizes that its protection extends to "private" communications "between two or more individuals," with the method or type of communications themselves playing a more incidental role.[57] Additionally, the Washington law prohibits not only interception, but also recording.[58]

For example, *In re Carrier IQ, Inc,*[59] the case involved numerous plaintiffs and claims under both the federal and state statutes discussed in this article.[60] The plaintiffs alleged that their cellphones came with a pre-installed software of which they were not aware and awareness of which

[49] 18 U.S.C.A. § 2511(d).
[50] *Id*.
[51] *See* WASH. REV. CODE § 9.73.030.
[52] WASH REV. CODE § 9.73.080.
[53] WASH REV. CODE § 9.73.060.
[54] 18 U.S.C.A. § 2515; WASH. REV. CODE § 9.73.050.
[55] See *id*.
[56] 18 U.S.C.A § 2511.
[57] WASH. REV. CODE § 9.73.030(1)(a).
[58] WASH REV. CODE § 9.73.080.
[59] *In re Carrier IQ, Inc.*, 78 F. Supp. 3d 1051 (N.D. Cal. 2015).
[60] *Id*. at 1059-61.

would have dissuaded them from purchasing their phones.[61] They further alleged that this software, called Carrier IQ, intercepted the following types of information from their phones: "(1) URLs (including… search terms, usernames, passwords, and GPS-based geo-location information); (2) GPS-location information; (3) SMS text messages; (4) telephone numbers dialed and received; (5) the user's keypad presses/keystrokes; and (6) application purchases and uses."[62] Because both the federal and Washington state statutes were implicated in the case, the differences in the court's analysis of the complaint are instructive here.

The district court analyzed the plaintiffs' ECPA claim in terms of (1) whether the purported interception was contemporaneous to the transmission of the communications in question; (2) which, if any, of the communications in the plaintiffs' complaint implicated the ECPA; (3) whether the purported interception occurred through the use of a device; and (4) whether the defendants acquired the contents of the communications.[63] The court sided with the plaintiffs on the first three issues but dismissed the complaint for failure to state a claim because the plaintiffs had not alleged that the defendants acquired the contents of the communications, and therefore, had not properly alleged a violation of the ECPA.[64]

By contrast, the court's Washington state interception analysis did not consider contents or contemporaneousness at all.[65] Additionally, the court reached different conclusions about which communications implicated each respective statute; while text messages were protected by both statutes, the federal act protected internet searches and the Washington act protected dialed phone numbers.[66] This result demonstrates that the differences between the two statutes are not merely cosmetic, but rather provide substantively different forms of privacy protection.

In addition to protecting different types of communications, the Washington statute requires different evidentiary showings than the Wiretap Act. As the Washington Supreme Court explained, a violation of the Washington law consists of "(1) a private communication transmitted by a device, which was (2) intercepted or recorded by use of (3) a device designed to record and/or transmit (4) without the consent of all parties to the private communication."[67] An electronic communication, therefore, need not be transmitted by a system affecting interstate commerce under Washington's statute. Instead, it must be 'private' and must be "between two or more individuals."[68] Private communications exist where parties

[61] *Id*. at 1060.
[62] *Id*. at 1062.
[63] *Id*. at 1076-90.
[64] *Id*.
[65] *Id*. at 1091-93.
[66] *Id*. at 1082-83, 1092.
[67] *State v. Roden*, 179 Wash. 2d 893, 899, 321 P.3d 1183 (2014).
[68] *In re Carrier Inc.*, 87 F. Supp 3d at 1093.

manifest an expectation of privacy, provided that the expectation is reasonable.[69]

The two acts also differ in their approach to what happens if only one party to a communication gives consent to an interception. Under the federal law, one party's consent is sufficient to provide a defense,[70] but this is not the case under Washington's statute. Under the Washington statute, all parties must consent to avoid liability.[71]

## IV. CHAT PREVIEW UNDER THE WIRETAP LAWS

Despite these differences, one key similarity between the federal and Washington state wiretap statutes is that neither statute adequately protects the privacy of consumers' thoughts from chat preview. The prospects of succeeding in a claim against a company using chat preview under either statute are grim considering both the letter of each law and their precedential history.

### *A. Chat Preview Under the ECPA*

Cases like *Rene* and *Ropp* suggest that keylogging devices and software programs generally do not violate the Wiretap Act.[72] In fact, *U.S. v. Barrington* explicitly states that keyloggers will only violate the act "if the signal or information captured from the keystrokes is . . . at that time being transmitted beyond the computer on which the keylogger is installed (or being otherwise transmitted by a system that affects interstate commerce)."[73] Much like keyloggers, chat preview functions capture keystrokes in real time. As such, the software captures what the customer types while it is still using "a system that operate[s] solely between the keyboard and the local computer,"[74] and therefore, does not capture electronic communications as defined in the ECPA.

Furthermore, the chat preview situations discussed in this article would seem to fit squarely into the ordinary-course-of-business exception to the Wiretap Act.[75] Such situations occur while a customer service agent is actively engaged in providing service to a client, after all. Furthermore, the ostensible purpose of the chat preview function is to increase the quality of customer service. Even if the use of chat preview itself is not a part of the ordinary course of the company's business, the chat software which features the chat preview function is undoubtedly a device furnished to a user as part of the ordinary course of business operations. Such devices

[69] *State v. Christensen*, 153 Wash. 2d 186, 193, 102 P.3d 789 (2004).
[70] 18 U.S.C.A. § 2511 (2)(d).
[71] WASH. REV. CODE § 9.73.030.
[72] *See Rene v. G.F. Fishers, Inc.*, 817 F. Supp. 2d 1090 (S.D. Ind. 2011); *United States v. Ropp*, 347 F. Supp. 2d 831 (C.D. Cal. 2004). Notably, In *Rene*, the fact that the captured keystrokes were made while the computer was connected typing e-mails did not convince the Court that the keylogger captured keystrokes from a system affecting interstate commerce.
[73] *United States v. Barrington*, 648 F.3d 1178, 1202 (11th Cir. 2011).
[74] *Rene*, 817 F. Supp 2d at 1094.
[75] *See* 18 U.S.C.A. § 2511(2)(a)(i) (2018).

are, by statutory definition, incapable of improperly illegally intercepting communications under the act.[76]

Claims under the federal statute will also face barriers because of the act's approach to consent, which only requires the consent of one party to a communication before an interception becomes lawful.[77] It is likely that a court might decide that (1) the company employing a chat preview function is a party to the communication and (2) that it implicitly consents to its own act of previewing customers' chat messages. This is to say nothing of the uncertainty in the statute as to whether a party to a communication can illegally intercept a message for which they were arguably the intended recipient in the first place. This ambiguity would seem to present threshold questions about (1) whether a person or company on an online chat with a customer is already a party to a communication if a message has not yet been sent and (2) if they are, whether that fact alone makes it legally impossible for them to unlawfully intercept such an unsent communication under the ECPA.

### *B. Chat Preview Under the Washington Wiretapping Statute*

The Washington statute seems at first glance to provide more protection to the customer, as it requires the consent of all parties,[78] but this apparent protection is likely illusory. A company could easily get around this requirement by embedding consent to chat preview in a lengthy terms of service agreement as a condition for using its chat service. Studies reveal that, when it comes to protecting their privacy, customers rarely rely on such agreements to set their expectations of privacy,[79] and such agreements are already commonly used to illicit customers' consent to other privacy invasions like installing spyware.[80] Indeed, since customers rarely even read these agreements,[81] it is easy for a company who wishes to access customers' private thoughts to obtain consent to intercept, record, and otherwise use customers' unsent messages however it wants. All the company would need to do is make a user click on a terms and conditions agreement before initiating a chat conversation with an employee.

This type of contractual consent is troubling, not just because it is a convenient workaround to subvert two-party consent, but also because it leaves customers inadequately informed and functionally deceived about the privacy of messages that they draft but decide not to send. Customers, having likely not read a terms and conditions agreement, may assume that

---

[76] 18 U.S.C.A. § 2510(5)(a) (2002).
[77] 18 U.S.C.A. § 2511(d) (2018).
[78] WASH. REV. CODE § 9.73.030 (2021).
[79] Woodrow Hartzog, *Website Design as Contract*, 60 AM. U. L. REV. 1635, 1636 (2011).
[80] *Id*. at 1647-48.
[81] Woodrow Hartzog, *The New Price to Play: Are Passive Online Media Users Bound by Terms of Use?*, 15 COMM. L. & POL'Y 405, 407 (2010).

an unsent message is invisible to all others, and with good reason. The existence of a "send" button, or an analogous feature in a chat window, logically implies that there is a step to be completed before a message is released from the sender's possession into the hands of the recipient. That step appears to provide a space for the editing, revision, and even last-minute cancellation of a message. In other words, the very fact that there is a final step which releases a message to the user on the other side of the chat creates a reasonable expectation that, until that step is completed, the customer is free to edit or even delete what they have written without the other person finding out about it. It is conceivable that this apparent failsafe against impulsively sending a regrettable message might even be an incentive for some customers to choose chat over in-person or telephone consultations, especially if the customer is upset and wants to avoid an unpleasant confrontation.

If a customer has chosen to communicate via chat for this reason, then chat preview threatens the very control over the conversation that the customer seeks to maintain. As Professor Woodrow Hartzog observed, this sort of "loss of agency and autonomy is probably the most deep-seated fear of users and the most pressing issue for policymakers."[82] Even in this era of ever-increasing data collection and privacy erosion, consumers should at least be able to assert agency over the decision whether to send their thoughts from the supposed privacy of their own device to another person or corporate entity who may then do whatever they want with the communication.

It is also more than mere conjecture or speculation to predict that the features of a chat window will influence a customer's expectation of privacy more than the contents of a terms of service agreement; rather, it is a logical conclusion from what we know about how users interact with the Internet. According to Hartzog, "[u]sers virtually never read the terms of use, yet they routinely use privacy settings. Thus, it is likely that website users will rely on representations made by significant features of website design more often than boilerplate terms of use."[83] What this means, in the context of an online chat with a chat preview function enabled, is that a user is not likely to think they are communicating until they hit "send" or perform some analogous function in the chat to officially send a message.

### *C. Privacy Risks of Chat Preview*

It bears repeating that, if a user thinks what they are typing is not visible to anyone else, then they have not yet truly typed a message or a communication, but rather the mere contents of their inward thoughts or feelings. Consider this dictum from the 9th Circuit Court of Appeals regarding the Fourth Amendment: "The express listing of papers 'reflects the Founders' deep concern with safeguarding the privacy of thoughts and ideas–what we might call freedom of conscience–from invasion by the

[82] Woodrow Hartzog, *On Questioning Automation*, 48 CUMB. L. REV. 1, 4 (2018).
[83] Hartzog, *supra* note 79 at 1661 (2011).

government."[84] This does not mean that chat preview as used in commercial contexts implicates the Fourth Amendment itself; clearly, it does not. However, it does suggest a person's right to be secure in their thoughts, to the extent that it exists, is not negated or waived merely by putting thoughts in writing. This would seem to nullify any argument that typing something into a chat window waives a reasonable expectation of privacy.

More importantly, this dictum points to an idea which is intuitive to most: there is something vitally important, perhaps almost sacred, about the right of a person to think candidly in the privacy of their own mind. Perhaps no violation of personal privacy could be more offensive to our basic conceptions of freedom than entering the private space of personal thought. The private realm of the mind is where we can consider, digest, and choose from among ideas freely, without the interference of coercive social pressures or the interests of third parties. The mind is perhaps the most private of all places, and therefore perhaps the space where a violation of privacy is the most troubling. The intrusion into privacy of thought by a private party may not be a constitutional violation, but it is still an intrusion on a right that the Framers of the Constitution thought to be important enough to codify in our country's most foundational legal code. Whether it is a private or government entity that violates that freedom is immaterial; in either case, a basic and fundamental facet of human freedom has been trampled.

Savvy users likely have some conception of the scale of data collection on the modern Internet. Although they may not know that cookies operate on the websites they visit to reveal their usage patterns to website operators[85] or that their data is aggregated into personal profiles and sold to advertisers,[86] they probably know that if they put something on the Internet, it can be found, retrieved, saved, and used by others. Furthermore, where no laws limit the length of time in which users' shared information can be stored, information about the user can be multiplied,[87] making the aforementioned profiles ever more scarily accurate and insightful in predicting a user's behavior, preferences, and personality. For users who value their privacy, the only recourse to address this fact may be to keep their thoughts to themselves and abort a post or message once they realize they do not want to expose it to mass data collection.

This last-minute decision not to post is not an uncommon situation; as a study conducted for Facebook by Sauvik Das and Adam Kramer demonstrates, this 'last minute self-censorship' is the rule, not the

---

[84] *United States v. Cotterman*, 709 F.3d 952, 964 (9th Cir. 2013) (citing *United States v. Seljan*, 547 F.3d 993, 1014 (9th Cir. 2008) (Kozinski, dissenting)).
[85] Jessica Lile, *Internet Privacy Regulations and the* Carpenter *Decision*, 87 UMKC L. REV. 777, 780 (2019).
[86] *Id*. at 789-90.
[87] Tsesis, *supra* note 1, at 441.

exception.[88] In fact, their study found that as many as 71% of users censor themselves at the last minute, at least some of the time.[89] Chat preview, therefore, eliminates an important mechanism by which many, if not most, users assert their right to keep their unexpressed thoughts private.

Some may argue that the consequences of this invasion will usually be fairly innocuous or even outweighed by the benefits of improving customer service and making agents' jobs easier. On the one hand, it is easy to see how knowing what a customer is typing before a message is sent can improve the quality of service, especially in the case of messages that are long, complex, or emotionally charged. Giving customer service agents a head-start on finding answers and providing service could improve the interaction for both sides. Additionally, if a customer is in the midst of writing an abusive, threatening, hateful, or otherwise inappropriate message into a chat, seeing it beforehand might allow an agent to end the chat before being subjected to such a message.

Yet, most of these benefits primarily apply to instances in which the customer will ultimately decide to send the messages in question. If an agent 'previews' written material that the customer then deletes, the legitimate benefits to the agent, if any, are minimized, while the violation of the user's privacy of thought is amplified and intensified. Indeed, if a customer drafts an inappropriate message and then erases it without sending it, the customer service agent is better protected by *not* previewing it.

Previewing instances of last-minute self-censorship may open the door to a multiplicity of possible abuses. These could come in the form of a rogue individual agent who records and saves an embarrassing display of emotion in order to use it against a client later, a company who sells potentially embarrassing information from an aborted message to advertisers, or even a third party who hacks or infiltrates the chat function to preview and expose the private thoughts of a political enemy. These risks offend basic American ideals of privacy and freedom of thought, even in the best of circumstances. However, chat preview does not represent the best of circumstances. There is an inherent asymmetry of advantage at play when Party A can preview Party B's messages, but Party B cannot do the same to Party A. This asymmetrical access to previews of the other party's messages exacerbates the risks of abuse.

To be sure, consumers can avoid these risks by refraining from chat communications, but this solution is only possible for those who are aware that they are being monitored as they type. Furthermore, leaving customers who have privacy concerns with no option but to refrain from chat features entirely might arguably restrict their access to customer service and have a chilling effect on the business-customer relationship. This outcome would be undesirable for both consumers and businesses.

All this is to say nothing of the potential applications of chat preview in interactions with government actors, which only serve to deepen the

[88] *See* Sauvik Das and Adam Kramer, *Self-Censorship on Facebook*, https://research.fb.com/wp-content/uploads/2016/11/self-censorship-on-facebook.pdf (page 1) (finding 71% of Facebook's users engage in this practice).
[89] *Id.*

privacy concerns already discussed. Consider, for example, the Washington case *State v. Townsend*.[90] In that case, police posed as an underage girl and communicated with the defendant by e-mail and instant messaging.[91] Unbeknownst to the defendant, the instant messaging program automatically recorded his correspondence with the fictitious teenager.[92] The defendant, unaware that he was in fact communicating with police, arranged a sexual rendezvous, whereupon he was arrested and charged with attempted second-degree rape of a child.[93] The Supreme Court of Washington held that the police had not violated the state wiretapping statute because the defendant had impliedly consented to the recording of communications.[94] The Court explained that e-mail users implicitly consent to the recording of the messages they send because e-mail does not work unless messages can be stored on the recipient's computer until the recipient can open them.[95] As for the instant messages, the court inferred implicit consent because the software had a privacy policy explaining that recording was possible in some versions of the software, and the defendant was presumed to be familiar with the policy.[96]

Now let us imagine that Mr. Townsend had communicated exclusively via instant messages with the police, and let us further assume that rather than sending the incriminating messages that arranged a meeting, he typed them out, changed his mind, and erased them. Yet, having perhaps obtained the fictional teenage girl's address, he decided to go to the address to apologize for his inappropriate behavior. Then, let us further assume that the police, having used a chat preview function in the chat software, saw the defendant type that he wanted to meet the girl for sex and went to the address to make an arrest. Under the Washington Supreme Court's reasoning in *Townsend*, all that would have been necessary to render the defendant's aborted message admissible in court would be an obscure clause in a privacy policy warning that some users may have access to chat preview.

Another important difficulty in addressing this area of law is that there is very little in the way of standard, broadly accepted legal terminology. As noted above, the various companies who market and sell chat programs have not agreed on a single term to describe chat preview, meaning that there is not even a standard industry term. Clearly, the wiretap statutes as written did not contemplate the development and popularization of chat preview functions and, as discussed, they provide little to no protection for consumers because of it.

---

[90] *State v. Townsend*, 147 Wash. 2d 666, 57 P.3d 255 (2002).
[91] *Id.* at 670-71.
[92] *Id.* at 671.
[93] *Id.*
[94] *Id.* at 676.
[95] *Id.*
[96] *Id.* at 676-79.

With both the dearth of protection afforded by federal and state wiretap statutes and the serious breaches of privacy that can occur because of chat preview in mind, there is clearly a gap in public policy that needs to be addressed.

## V. THE ECPA AND WASHINGTON STATE STATUTES SHOULD BE AMENDED TO ACCOUNT FOR CHAT PREVIEW

To better protect the privacy of users' thoughts, federal and state wiretap legislation should be amended to require a party wishing to employ chat preview to do the following: (1) notify the other parties to the communication and obtain their consent prior to initiating the preview function; (2) not rely on any consent, explicit or implied, given prior to the initiation of the communication in which the preview is to be employed; and (3) cease previewing the chats of any party who withdraws consent at any point during the course of the communication.

The first two requirements are necessary because of the deeply flawed provisions of the current statutes regarding consent. Simply put, regarding privacy policies and other clickwrap or browsewrap terms of service agreements as legally binding consent ignores the reality of how users interact with the Internet. Despite the conventional wisdom that it is unwise not to read something before agreeing to it, the FTC has found that online customers tend to recklessly accept online agreements either out of irrational confidence or a desire for instant gratification; as a result, people simply do not read these agreements.[97] The sheer length and number of these agreements presents another obstacle to getting customers to read them; according to one study, the average American would need to spend 201 hours each year just to read the privacy policies for all the websites they use.[98] Even if a user were to invest that time, there is no guarantee they would even understand the terms of the agreement—as Cheryl Preston observed, "[w]rap contracts are increasingly elaborate, monotonous, and written in ways that suggest the drafter intended to obfuscate the scariest parts by embedding them in excess verbiage and repetition."[99] The consent obtained by these contracts is made even more dubious by the fact that they are not negotiable,[100] meaning that users are made to choose to either fully surrender their privacy or be excluded from a company's online services outright.

This proposed amendment to the wiretapping legislation would give users an opportunity to decide whether to consent to chat preview, not in a vague and abstract way, but directly and in the moment. It would not permit companies to obtain blanket consent to the use of chat preview well in advance of the actual conversations between customers and customer service agents. This would maximize the customer's opportunity to

---

[97] Cheryl B. Preston, *"Please Note: You Have Waived Everything": Can Notice Redeem Online Contracts?*, 64 AM. U. L. REV. 535 564 (2015) (citing FED. TRADE COMM'N, NEGATIVE OPTIONS: A REPORT BY THE STAFF OF THE FTC'S DIVISION OF ENFORCEMENT ii-iii (2009)).
[98] *Id.* at 553.
[99] *Id.*
[100] *Id.* at 553-54.

decline having their unsent thoughts monitored. The notice requirement would also give customers an idea of how and when their chat messages are being previewed. Without understanding this information, customers may have difficulty making an informed decision regarding whether to consent to the preview.

Furthermore, the termination requirement allows customers to reassert their right to privacy of thought if they change their mind about waiving it. Consider some of the reasons given by the Das and Kramer Facebook study for last-minute self-censorship: "(1) Users did not want to instigate or continue an argument; (2) users did not want to offend others; (3) users did not want to bore others; [and] (4) users did not want to post content that they believed might be inconsistent with their self-representations."[101] Many times, a conversation may escalate from a fairly normal interaction to an argument or emotionally charged exchange. In these situations, customers may not feel a need to assert their right to privacy of thought until the situation begins to escalate. While the termination requirement may burden customer service agents by making them operate with less knowledge of the customer's emotional state, it could save the customer from embarrassment.

These requirements also address the inherent power imbalance in customer-business interactions employing chat preview. Customers are usually singular actors with limited resources, whereas companies have entire teams of employees and vast resources. Also, customers who need help or redress for a complaint often do not know the company's policies or the full details of its bureaucracy. These are clear advantages that companies have over their customers where a customer has a complaint or dispute with them. These advantages are further entrenched and enhanced by the fact that most disputes between customers and businesses are settled by companies' internal mechanisms as opposed to litigation or arbitration.[102] "Thus," as one scholar put it, "[t]he design and execution of corporations' internal complaint systems are largely disconnected from legal rights."[103] Adding the chat preview card to this already stacked deck gives customers even less power in disputes with companies, as it allows businesses to get inside the customer's head and strategize in a way that the customer is unable to do.

However, this proposal stops short of a whole-sale ban on chat preview. One reason for this is an acknowledgement of the real benefits that chat preview can provide to companies and customers alike. While it is easily abused in situations where a customer has a dispute or grievance with the company on the other end of the chat, its risks are decidedly reduced in more mundane customer service situations. When a customer simply has questions or needs to access some common, everyday service,

[101] Das, *supra* note 88.
[102] Rory Van Loo, *The Corporation As Courthouse*, 33 YALE J. ON REG. 547 548-49 (2016).
[103] *Id.* at 555.

they are likely to appreciate the increased speed and efficiency of service that is made possible by chat preview.

Furthermore, because the keystroke tracking technology behind chat preview is "plain old Web 1.0,"[104] as opposed to some new and highly technical interface, overly aggressive regulation would be unwise. To truly make it impossible for companies to key log and read customers' unsent messages with chat preview, it would probably be necessary to substantially burden the use of JavaScript itself. This could create enormous strain on the very fabric and infrastructure of the Internet itself, as JavaScript is a standard building block of web design[105] and is widely used by companies ranging from Apple and Google to Firefox in their browser software.[106] To be certain, the potential violations of user privacy that we have discussed are grave and deserving of remedial action, but that concern for privacy must be balanced against the costs of regulation and the useful and desirable features that customers may stand to lose if regulation is too far-reaching.

This proposed amendment seeks to properly balance these important considerations by specifically targeting chat preview as a practice rather than broadly regulating its versatile and ubiquitous enabling technology. It does not require the customer's consent to all the Javascript-enabled features of a chat or website, nor does it give them the right to request termination of all such features. Rather, it is limited only to the specific features that allow the agent on the other end of the conversation to monitor unsent messages. Additionally, the burdens of complying with this proposed amendment should be minimal for most companies. Rather than uninstalling or eliminating their current chat service and buying new chat software, turning off chat preview can be as simple as going into the settings of the chat program and clicking a button.[107] In fact, some chat preview providers even include instructions on their websites on how to do this.[108]

That is not to say that this is a perfect proposal by any means. For one thing, as discussed above, unsent chats may not meet the federal statutory definition of 'electronic communications' because intercepted keystrokes are not being transmitted by a system that affects interstate commerce. Because of this fact, this proposal seems to create a narrow exception to the statutory definition of electronic communications without providing much explanation for why keystrokes should be treated in a substantively different way in chat scenarios as opposed to any other circumstance. Admittedly, the proposal seems to fit more comfortably into the framework of the Washington statute, the protection of which is not limited by the impact of a particular communication system on commercial markets.[109]

---

[104] Vaas, *supra* note 15.
[105] *See id*.
[106] Dirk Grunwald, *The Internet Ecosystem: The Potential for Discrimination*, 63 FED. COMM. L.J. 411, 421 (2011).
[107] *Real-time typing view, supra* note 5.
[108] *See id.*
[109] *See* WASH. REV. CODE § 9.73.030 (2021); *compare* 18 U.S.C.A. § 2510(12) (2002).

However, rather than creating an irrational incongruence in the federal law, this proposal could alternatively be seen as the first step toward greater reform and protection of consumer privacy. This article does not pretend to propose a full regime of privacy legislation or reform, but its analysis of chat preview does reveal serious deficiencies in the current statutory regime, and if amendments designed to address the risks of chat preview prompt further refinements and reforms to improve the law, then that would be a welcomed development.

Another possible criticism of the amendments proposed by this article is that they are not based on concrete harm suffered by actual consumers, but instead, upon the possibility of some harm. Proposing changes to the law based on what could happen as opposed to what has happened may seem rash to some. Certainly, the mere fact that unsent or even 'last-minute self-censored' chats *may* be recorded, sold, or used against a customer is not in itself proof that such things *are* happening. There may even be some truth to the idea that companies might be incentivized not to abuse chat preview because they do not want to risk losing their customers' trust. However, preventing harm in the future is a major function of law, if not the entire point of it. Even if certain companies are not presently abusing chat preview to the detriment of their customers, the proposed amendment would be an effective and needed deterrent against them ever beginning to do so.

Furthermore, this criticism ignores the fact that one of the most problematic elements of chat preview is the fact that the person on the other end of the chat does not know that it is happening. If a customer does not even know that their unsent messages have been intercepted and seen, they will be unaware of the harm that could result from the interception. This does not mean, however, that no harm has occurred. Even for those who are unconvinced that the initial privacy invasion of chat preview is a harm in and of itself, any sale or other disclosure of the contents of previewed messages to a third party expands the circle of people with access to the customer's private thoughts without the customer's consent. The more that circle increases, the greater the violation of the customer's privacy becomes and, thus, the more serious the harm suffered becomes.

The fundamental importance of protecting the privacy of personal thought cannot be overstated in this conversation. The mind may be the only completely private space, the only place where a person can truly form independent thoughts, feelings, and a sense of identity without the intervention of concerns about the judgment of others. Privacy of thought is the singular and ultimate protector of individuality, the one space where neither the law nor the pressures of the outside world or culture can inhibit, punish, or restrain a person from being as they are. In this way, private thought is arguably a necessary precursor to other fundamental rights like freedom of expression and freedom of conscience. The narrow, limited tailoring of this proposal to chat preview situations and its reticence to

advocate for broader or more burdensome requirements is a concession to concerns about the speculative nature of chat-preview-facilitated harms, but only limited concessions are acceptable because of the great importance of the individual right at stake.

## VI. CONCLUSION

### *A. Summary*

Chat preview is a potentially useful tool for businesses who provide customer service online, but it is also a potentially dangerous one for the customers on the other end of the chat. The danger, brought on when customers effectively brainstorm messages to send and edit as they operate out with the mistaken belief that their typing will not be seen, is an intrusion on a fundamentally important right of all people: the right to privacy of thought.

The most analogous intrusion of privacy, wiretapping, is regulated at both the state and federal levels, but customers subject to chat preview can have little hope of redress in court under either the ECPA or the Washington State wiretapping statute. While customers face different obstacles under each statute, both statutes present substantial barriers to relief, especially in cases where consent to the use of chat preview may be implied from language in a company's privacy policy or their website's terms of service contract. Because of this, amending the wiretapping statutes is a necessary measure to ensure the integrity of user privacy and protect customers from unwanted intrusions into their private thoughts as typed, but not sent, in a customer service chat window.

The wiretapping statutes should therefore be amended to require (1) in-the-moment disclosure by the party intending to use chat preview and in-the-moment consent by the party to be previewed, (2) a prohibition on relying on privacy policies or terms of service agreements to furnish consent, and (3) a requirement that the party using chat preview cease using it upon the request of the previewed party. Such an amendment would balance the importance of the implicated rights with concerns about overregulation and legislative overreach and provide necessary protection for consumers while not demanding that businesses re-invent the technological wheel for providing customer service to their clients.

### *B. Moving Forward*

Technology is advancing at a blistering pace, and the speed at which legal issues arising out of innovation emerge is equally rapid. Although there are many exciting opportunities presented by new technologies like chat preview, there are also many potential dangers, especially to user privacy. This is true not only of chat preview functions, but also of a litany of other services and features that have or will become commonplace parts of everyday life.

This article has purposefully limited its scope and resisted the urge to make broad proclamations and proposals about the broader area of online privacy because it is such a complex and multi-faceted issue. As the Internet becomes ever more omnipresent in people's lives, the number of privacy-implicating interactions grows ever larger and the issues surrounding privacy become ever more complex. Properly thorough treatment of the boundaries of the individual right of privacy would require extensive research of the kind that is better suited to a full-length work.

However, this does not mean that further work and research should not interrogate the larger, more general questions about what privacy means in today's highly inter-connected landscape. The rapid forward march of technology may soon make it impractical to make privacy-related policy on an issue-by issue basis. Instead, it may be necessary to develop more basic, bedrock principles regarding the nature and extent of people's right to privacy online, especially as it can be enforced against private actors. Without a basic, consistent, and coherent understanding of the expectations of privacy that people are entitled to when they go online, we risk creating labyrinthine and self-contradictory policies that create random and unpredictable protections for users and place inconsistent burdens on businesses. This discussion will necessarily implicate judicial precedent and existing law, but it may also require deeper discussions into what the purpose of the law is, what lengths we are willing to go to protect individual rights against both state and private actors, and how technology shapes and modifies those rights.