Colin Hehn
August 24th, 2023
CS:3640
A1 Write-Up

When Privacy in Tech Reaches Legislation

What is the United Kingdom's "Online Safety" bill, and what does it mean for us?

In an ideal world, security online and an appearance in modern media exist as mutually exclusive cases. When everyone is talking about a celebrity's new kid or a political candidate and not SQL injection, some sort of peace has been achieved. A good ninety-nine percent of the time they swoop into the public eye is when there has been a breach of some kind, leaving the public feeling a bit disturbed, and maybe even wronged. These cases arise most of the time from a security flaw, something where a member of the public figured out a way to crack the safe. However, it becomes a completely different story when the perpetrator of such an *attack* is sitting in Parliament instead of behind a computer screen. In April of 2019, the government of The United Kingdom took a stab at internet regulation with "The Online Safety Bill," a piece of legislation designed to make the country the "safest place in the world to be online" (Porter, 2023). Four years later, the can has been kicked far down the road by COVID-19 relief and excessive changes in the cabinet, though now with many new proposed components, making it an incredibly hefty ask of the world's tech companies and the users of the applications they oversee. Calling it an *attack* may be some overzealous word choice, though it would not be wrong to say that such laws would endanger the online safety of all UK residents.

The part of the bill that's particularly problematic targets messaging apps, and not only the kind that is implicit to your phone, like iMessage or Google Messages, but those existing online and the app store as well, such as WhatsApp or Facebook. When someone sends a

message to another person using these applications, the message is encrypted in such a way that only the sender and receiver are able to read its contents. Not even the company itself can intercept and read the contents of the message, which also means that your local or federal government, or any of its affiliated organizations, cannot read it either. This sounds alright, unless you really want your mayor to know about the cool TikTok you sent your friends last night. For the average upstanding citizen, having this sort of privacy and security seems like a basic right, as I can't imagine many folks would be fond of people peeking in on their lives. However, for those who aren't exactly making an honest living, this encryption appears as less of a right and more as a tool for their back alley trade. This idea is what the UK Parliament is attempting to crack down on. Page 106 of the bill reads, "Use accredited technology to prevent individuals from encountering CSEA content, whether communicated publicly or privately," (UK Parliament, 2023). CSEA, when used in the context of this document, stands for Child Sexual Exploitation and Abuse offenses; just going off of the acronym, one shouldn't have to elaborate on why users shouldn't be exposed to this type of content online, especially when a user is under the age of eighteen, let alone eight and a half. The lawmakers have their heads in the right place; many, if not all, of these messaging applications have become mediums for devilish behavior, as being able to contact others around the world for black market activity quickly, and *securely*, is too good of a service to pass up. Wanting to curb this type of online application use case is what I believe many around the world would see as a valiant initiative. Whether that is possible without compromising the functionality of the entire user base is a whole different ball game.

To dig a little deeper into this, we'll explore where WhatsApp, a free, cross-platform messaging and voice-calling application, fits into the mix. WhatsApp, now owned by Meta, is

the largest piece of social messaging software on the planet, netting just over two billion users worldwide. Their (faster than the) elevator pitch, as directly quoted from the landing page on their website, is "Simple, reliable, private messaging," with a highlight on their end-to-end encryption use being made only a brief scroll down. With security and privacy being especially integral to their application ecosystem, it's no surprise that the company isn't all that thrilled with the Online Safety Bill. In fact, in a letter addressed to the Parliament of the United Kingdom, they stated that the organization would withdraw from the country altogether should the bill be passed in its current state (Porter, 2023). But what *exactly* in this legislation is appalling the executives at the social messaging giant so much to make them give up an entire 67.33 million users (Google, 2021)? Perhaps the answer lies in the technological infrastructure powering the company and its success worldwide in the first place.

WhatsApp is predominantly built on Erlang, a general-purpose, concurrent, functional high-level programming language that came out in 1986. A few of the other driving forces in their technical stack are PHP, an open-source, scripting language also used in the creation of sites like YouTube, and XMPP, otherwise known as the Extensible Messaging and Presence Protocol. XMPP, based on XML, a popular data transmission markup language, provides the backbone for the service and enables the *instant* messaging feature that everyone knows and loves. On that same note, whenever someone sends a message on WhatsApp, it is first converted into what we humans see as random jargon via encryption, before being sent to its intended recipient via the protocol mentioned prior, where it is then converted back to legible text or image data via decryption. The *key* used to encrypt this message, or the piece of information needed for encoding and decoding the data you want to send to your colleague, only exists on your device and your colleague's device. The same applies to when your neighbor wants to send a message to

their significant other, or their kid; the key used to transmit the text they're sending *securely* only exists on their phone, and their chosen recipient's phone. WhatsApp uses Signal Protocol, a cryptographic protocol developed by Open Whisper Systems, to achieve this alongside many other companies, like Google, who just implemented end-to-end encryption in their own home-brewed messaging app that comes pre-installed with most Android phones. The specific algorithms Signal Protocol uses to provide these encryption features to some of the world's largest organizations include X3DH, Double Ratchet, Sesame, XEdDSA, and VXEdDSA, which each bring something of their own to the table, like key sustainability (later keys can't be used to figure out old ones), and multi-device encryption sessions. We won't dig into how each one functions in this exposition, however, so do feel free to look into those at your leisure.

The Parliament of the United Kingdom proposes to add functionality to WhatsApp that would undermine the efforts of these encryption techniques. What exists right this moment as a way for law enforcement agencies and beyond to obtain access to these initially private messages for the purpose of justice, is a request-based system, and one that's strictly *reactive*. Many companies conduct this application and law enforcement relationship differently; one in particular that you may have heard about is the Apple vs. FBI San Bernardino case. A suspected member of a terrorist organization's phone was seized by the authorities, though the FBI was without a way to access the data held within it. They insisted that Apple unlock the phone and that it would be a one-off case, though Apple refused, leading to one of the largest big tech and government clashes to date (Kharpal, 2016). WhatsApp has shown us a mildly different approach, where they instead "carefully review, validate and respond to law enforcement requests based on applicable law and policy" (WhatsApp, 2021). This take on consumer data privacy doesn't directly jeopardize the digital well-being of the entire population, and operates in

what I believe to be a similar manner to the police requiring a search warrant in order to enter one's home. A protocol like this one won't stop crime as it's being committed, however. In order to monitor and shield users from this CSEA (Child Sexual Exploitation and Abuse) content, UK lawmakers seek to have tech companies, like Meta, put in place mechanisms to *proactively* detect it as it's sent, whether it be public or private. Unfortunately, this sort of defeats the purpose of the end-to-end encryption in the first place, and I'm sure many tech executives were left with a sour taste in their mouths. WhatsApp, in particular, made it known to the British government that this detection mechanism was something they would not be willing to include in their application.

Ultimately, this left all those who are for the Online Safety Bill to search for alternatives, ones that would allow for the *proactive* detection of harmful messages sent over United Kingdom networks, though come without the need to dismantle the encryption protocols that the communications company has in place for their service, just as many other organizations do as well. The collective thought led to the concept of client-side scanning for CSEA content, which would provide this message detection functionality, though still leave everything encrypted in transit. Despite this, at the surface level, accomplishing what was required of WhatsApp to accommodate the potential new public policy, the company determined that this would still fatally undermine end-to-end encryption. "Proponents say that they appreciate the importance of encryption and privacy while also claiming that it’s possible to surveil everyone’s messages without undermining end-to-end encryption,” the company's open letter states. “The truth is that this is not possible” (Cathcart, 2023). Conceptually, we are left at a standstill, as there is now no existing, and viable, method of CSEA content detection that can work in the context of the WhatsApp application's intended function.

The British government's next move is unclear at this time. In that same open letter from Will Cathcart, head of WhatsApp at Meta, and many other prominent names of the tech industry, the executives insist on Parliament urgently rethinking the bill, and "revising it to encourage companies to offer more privacy and security to its residents, not less" (Cathcart, 2023). So what's the path forward, and what can one expect to take place as we dive deeper into the months of fall? Well, this imminent threat to end-to-end encryption isn't the only thing many see wrong with the bill. Matthew Lesh, the head of public policy at the Institute of Economic Affairs, highlights that there's a massive disparity between what is okay for children to see online and what's okay for adults included in the potential legislation (Lesh, 2023). This leads to the question of whether we make all users verify their age, leading to a plethora of consumer privacy and data protection issues, or filter content for everyone and moderate the internet as if everyone were a child. Neither sounds like the greatest of options, at least from where we stand right now. Luckily for all of the residents of the United Kingdom, the bill isn't in a completely finished state. It's being debated in the House of Lords, the second chamber of the UK Parliament, and may (hopefully) return looking a bit different than we remember. After this deliberation and a few more round trips through the chambers of government, the laws will be put in place. The UK's Department for Science, Innovation, and Technology will be working with Ofcom, the Office of Communications, to "lay the groundwork for the laws to be enforced once they are introduced" (Guide to the Online Safety Bill), and will be using a phased approach, focusing on addressing the most serious online harms first.

This paper isn't to say that there aren't promising components of the Online Safety Bill, because much of it brings into legislation processes that will be of astounding support to children's charities, one of the main proponents of the policies, let alone the youth themselves.

The internet remains a relatively unconquered frontier, and some kudos are due to the UK Parliament for taking it upon itself to eliminate a lot of bad behavior online, especially when it comes to those who haven't even graduated high school. That being said, there is such a thing as taking too big of a first step, just as was done here with some over-the-top guidelines and unforeseen dangers to consumer privacy and security. All that's left to do is wait and see what the final product looks like, as that will directly affect the chances that we see similar policies pop up in other countries around the world as well.

References

- "Apple V. FBI." *EPIC - Electronic Privacy Information Center*, epic.org/documents/apple-v-fbi-2.
- Cathcart, Will. "An Open Letter." *WhatsApp*, 17 Apr. 2023, blog.whatsapp.com/an-open-letter. Accessed 28 Aug. 2023.
- "Documentation." *Signal Messenger*, signal.org/docs.
- "FAQ." *WhatsApp*, 2021, faq.whatsapp.com/820124435853543. Accessed 31 Aug. 2023.
- "A Guide to the Online Safety Bill." *GOV.UK*, 30 Aug. 2023, www.gov.uk/guidance/a-guide-to-the-online-safety-bill.
- Kharpal, Arjun. "Apple vs. FBI: All You Need to Know." *CNBC*, 29 Mar. 2016, www.cnbc.com/2016/03/29/apple-vs-fbi-all-you-need-to-know.html.
- Lesh, Matthew. "A Harmful Approach to Harmful Content | Matthew Lesh | the Critic Magazine." *The Critic Magazine*, 17 Jan. 2023, thecritic.co.uk/a-harmful-approach-to-harmful-content.
- Nivesararao. "WHATSAPP — Technology Stack - Nivesararao - Medium." *Medium*, 15 Dec. 2021, medium.com/@nivesararao2700/whatsapp-technology-stack-3fbb4b76e130.
- "The Online Safety Bill." *UK Parliament*, 26 July 2023, bills.parliament.uk/bills/3137. Accessed 31 Aug. 2023.
- Panghal, Amit. "WhatsApp's End-to-End Encryption, How Does It Work?" *Medium*, 8 May 2019, medium.com/@panghalamit/whatsapp-s-end-to-end-encryption-how-does-it-work-80020977caa0.

- Porter, Jon. “The UK’s Online Safety Bill, Explained.” *The Verge*, 4 May 2023, www.theverge.com/23708180/united-kingdom-online-safety-bill-explainer-legal-pornography-age-checks.
- Thadani, Trisha, and David DiMolfetta. “U.S. Tech Companies Say U.K. Privacy Bill Poses ‘Serious Threat’ to Communication.” *Washington Post*, 1 Aug. 2023, www.washingtonpost.com/politics/2023/08/01/us-tech-companies-say-uk-privacy-bill-poses-serious-threat-communication.
- Volpicelli, Gian M. “All That’s Wrong With the UK’s Crusade Against Online Harms.” *WIRED UK*, 9 Apr. 2019, www.wired.co.uk/article/online-harms-white-paper-uk-analysis.
- Wallis, Jerry. “WhatsApp Tech Stack Explored — the Tech Behind Series.” *WEBO Digital*, 5 Apr. 2023, webo.digital/blog/whatsapp-tech-stack-explored.
- “What U.S. Policymakers Can Learn From the U.K.’s Online Safety Bill | Brookings.” *Brookings*, 18 May 2022, www.brookings.edu/articles/what-u-s-policymakers-can-learn-from-the-u-k-s-online-safety-bill.