We Hope You Won't Notice:

Risk Management and Secure Communications

What Some Communications Providers are Shy About Divulging. Why It's Time to Expect More.

LUNAR PRIVACY

Control:

When it comes to data security, more direct control doesn't just feel better. It really is better.

Maximum control over critical data pleases a first-tier information security professional. For secure communications in particular, you probably value authentic end-to-end encryption, or insulation from third-party assets, or fierce gatekeeping – curbs on access. All more than reasonable, and achievable today.

But if you're on top of your security game, when you scrutinize some of the big names astride today's secure communications landscape, the queasier you feel.

Secure mobile communication and collaboration solutions are here to stay. The post-pandemic workplace will probably never snap back to its office-bound, pre-2020 state. In all likelihood the information workforce is permanently distributed, firing sensitive information across time zones and between continents around the clock. (More than a few Silicon Valley tech leaders have moved away from California to run things *in absentia* – in Meta's case, from Tel Aviv or London.[1]) Mobile app security must support this new normal. In the past decade, well-known BCPs (business collaboration platforms) such as Slack™, Dropbox,™ WhatsApp™ and Skype™ have become go-to, high-functioning aids to worldwide business and personal workflow.

But some big names offer their customers a level of control some experts call disturbingly insufficient.

As food for thought, here is a glimpse of two important forms of control dilution: vulnerabilities the big household-name BCPs hope you, the security-conscious, control-minded decision maker, won't notice. The first is technological. The second is about devils hiding in terms-of-service details, and the level of security and privacy you actually get when you click I AGREE. (Spoiler: less than you expect.)

First, the technology issue. When a communications platform integrates third parties to deliver on lofty promises of versatility, reach, availability or economy – those parties may include remote servers, apps, or something else – customer control over data can be a casualty. Who evaluates those third-party resources stitched together to achieve service or functionality promises? And against what standards?

In a 2022 paper, University of Wisconsin-Madison researchers found that Microsoft Teams and Slack, among other, similar business collaboration platforms, "have fundamental issues in their handling of third-party apps," as a summary in *Wired* put it.

This is how *Wired* covered the researchers' findings about these particular BCPs:

> They both allow integration of apps hosted on the app developer's own servers with no review of the apps' actual code by Slack or Microsoft engineers. Even the apps reviewed for inclusion in Slack's App Directory undergo only a more superficial check of the apps' functionality to see whether they work as described, check elements of their security configuration such as their use of encryption, and run automated app scans that check their interfaces for vulnerabilities… All of that leaves users—who have grown accustomed to more well-secured third-party app environments, such as the code reviews implemented in Apple's App Store and Google Play—vulnerable to risks they don't expect.[2]

In their paper, the researchers themselves wrote:

> Beyond basic chatting features, modern BCPs usually offer many third-party integrations, commonly known as apps, which are cloud services providing additional productivity – enhancing functionalities in the workspace, often connecting users' data from other services (such as email or online storage) to the workplace. These BCP apps **exist on cloud servers not maintained by the BCP**. These app backends communicate with the BCP servers by subscribing to event notification APIs and reacting when information about a new event is received. The widespread usage of BCPs in remote work environments implies that a lot of sensitive information passes through it. With the potential ability to access such information, BCP apps lead to security and privacy concerns … **preventing further issues requires redesigning the BCP app access control model.**[3] (Emphasis ours.)

Now, insufficiently vetted third-party apps have been a known sore point in computing since forever. You would think business software covering more sensitive, critical missions should be held to higher standards, and you'd be right. But a 2021 survey by CyberRisk Alliance Business Intelligence found 91% of U.S. IT and cybersecurity decision makers had endured a recent security incident attributable to a third-party technology resource or partner.[4]

Slack is not only deemed vulnerable on the third-party question, but is by any measure enormous; the company claims 77 of the Fortune 100 companies use Slack Connect. Slack's sheer heft, 10 million daily active users by some estimates, presents bad actors in cyberspace with a large and tempting attack surface. "Slack has become a platform where users must be vigilant about looking out for phishing attacks and spam messages," warned security analyst Joel Witts in March 2023. "Because Slack is invite-only, users assume that their workspace is secure, but this is not always the case."[5] Cybersecurity innovators like Avanan and SafeGuard Cyber have developed custom, Slack-centric security platforms to try to mitigate Slack's vulnerabilities.

Slack is fond of portraying itself as a "default standard" in secure communications, flaws and all. "Slack is committed to helping companies like IBM, T-Mobile, and Target build a digital HQ so they can thrive in this new era of work," says the company.[6] But must customers resign themselves to ongoing, disquieting security and control issues, such as those raised by the University of Wisconsin research team, in order to get seamless connectivity and information-sharing over distance? Is this the best "default standard" the industry can come up with?

Before you answer, consider a second form of control dilution. This one has nothing to do with third parties;

it concerns assurances from the provider itself, and an alarming gulf between promises and reality.

Not long ago, it was widely believed that WhatsApp, launched in 2009 and bought five years later by Facebook parent for a princely $19 billion, provided end-to-end data encryption as an integral feature. An online search readily turns up a trove of privacy experts saying so. On this and other fronts, the company projects a good privacy game. Soothing disclosure language from WhatsApp assure users that they retain total control over their own metadata. "You are in control," states boilerplate text in the WhatsApp online help center. "Our additional privacy features, such as setting your messages to disappear or controlling who can add you to groups, give you an added layer of privacy."[7]

The whole truth about WhatsApp is a little different. An extensive, deep-dive 2021 deep-dive investigation by ProPublica, the nonprofit newsroom, reported that WhatsApp is "far less private than its users likely understand or expect… Facebook has quietly undermined its sweeping security assurances in multiple ways."

ProPublica said while WhatsApp privacy settings *seem* to indicate users control their own metadata – meaning they are allowed to decide if only contacts, everyone, or nobody can see your profile photo, status, and when the app was last opened, among other things – user data is *actually* collected, analyzed, and perhaps monetized by Meta, regardless of what settings a user selects.

It's not actually encrypted end to end, according to ProPublica – not the way an information security professional understands the term, anyway. WhatsApp keeps hundreds of content monitors at work around the clock, probing private user content as it slides by, looking for illicit material and sometimes sharing it with law enforcement. None of that is mentioned in the WhatsApp Terms of Service.[8]

ProPublica's findings were corroborated recently in a privacy analysis performed at the Center for Identity at the University of Texas. The headline finding, relayed by Diggit magazine in January 2023: "WhatsApp, as part of the umbrella company Meta, mines, collects and shares users' private information and shares it with third parties."[9]

For data owners, not exactly the epitome of control.

They can't get away with it, can they? Not after those definitive-sounding assurances about privacy. But they can if users agree to it – and whether they know it or not, they have.

Embedded deep within the 3,700-word WhatsApp Terms of Service users must accept in order to access the platform is this lawyerly sentence: "In order to operate and provide our Services, you grant WhatsApp a worldwide, non-exclusive, royalty-free, sublicensable, and transferable license to use, reproduce, distribute, create derivative works of, display, and perform the information (including the content) that you upload, submit, store, send, or receive on or through our Services."[10]

If you're using WhatsApp to trade "private," proprietary notes about a prototype product still on the drawing board – a breakthrough pickup truck or a new variety of canned soup – that sentence literally assigns Meta the right to make a movie about it. Negotiating a pro athlete's contract or a class-action lawsuit settlement? Same deal.

How private is that? Not very. Then again, how many WhatsApp users, or even enterprise CISOs, scour the Terms of Service during the signup process? Meta and WhatsApp make it easy not to. The setup sequence allows them to affirm they've read the Terms of Service by clicking an AGREE button on a separate screen, whether they really have or not. Admit it: virtually all of us, speeding through some process in cyberspace, tick the "I read and

understand…" box in situations like this without doing either. Sometimes it's a harmless act of omission. In this case it makes business users an on-the-record accessory to massive control dilution.

Some users have caught wind of these profound data-control issues and rebelled, transferring their loyalties elsewhere. Regulators overseas have sanctioned WhatsApp for falling short of required transparency obligations; the European Data Protection Board (EDPB) levied a €225 million fine.[11] But the risk environment remains mostly unchanged; WhatsApp is under pressure to make money. ProPublica obtained a December 2022 sales presentation putting user privacy in actual, if distressing, context. It said the app's owners will "open the aperture of the brand to encompass our future business objectives. While privacy will remain important, we must accommodate for future innovations."[12]

It is old hat at this point to chirp that if you're not paying for a product, you're the product – and a number of popular BCPs, including WhatsApp, are free. It is a little newer observation to say that participating in such a data ecosystem – essentially, ceding control of your information in return for convenience or value – makes you a bit player in a mushrooming "surveillance capitalist" system.

The term was coined in the 2010s by Harvard professor and social psychologist Shoshana Zuboff. In surveillance capitalism, she says, the more you (or any business) know, the more powerful you are – so there's a certain economic logic to accumulating information by any means possible. (And a lot of high-value information flows through leaky BCPs. A 2021 Veritas Research survey found 68% of U.S. knowledge workers share sensitive and business-critical company data over business collaboration platforms, even though 39% said they had been reprimanded for doing so.[13]) The profit-and-power motive power driving surveillance capitalism explains in a nutshell why Big Data keeps getting bigger, even though, in Zuboff's estimation, it adds up to "an overthrow" of private dominion over private, owned information.[14]

Lunar Privacy wants you to keep control of your information, even though it means abstaining from feeding surveillance capitalism.

You almost certainly need mobile secure communications. But you almost certainly don't want the compromises laid out in these pages: third-party servers with unknown cybersecurity safeguards, hosting your data in unknown locales. Unvetted apps on the system, providing attack vectors for malefactors. End-to-end encryption that isn't as end-to-end as you thought. Unwittingly clicking away

exploitation rights to your own privileged information. The truth is, Lunar Privacy makes it possible to have the convenient upsides of mobile secure communications without these glaring downsides.

The University of Wisconsin-Madison survey of BCP technical vulnerabilities concluded, "[Preventing further issues requires redesigning the BCP app access control model." Lunar Privacy has done exactly that. Not just access controls but the collaboration platform, data storage, and secure network protocols. The result is Lunar Fusion, Lunar Connect, and Lunar Encrypt: a complete, integrated suite of managed secure mobile communications services.

It delivers risk mitigation with no compromises in functionality or usability. No X-factor third parties; true end-to-end encryption; no data visibility for anyone except you and those your authorize. Sharing leadership with technology proven for years in highly sensitive public-sector, intelligence, and law enforcement settings, Lunar Privacy is suitable for the most demanding private sector missions.

Some big-name secure communications come standard with attributes or loopholes they hope you won't notice. At Lunar Privacy we hope you'll notice everything.

Finally, you're not in the dark.
You're not the product.
You have control.

Contact us to hear more.
info@lunarprivacy.com

LUNAR PRIVACY
One mission. Secure communications.

Endnotes

1 Sheera Frenkel and Mike Isaac, "Mass Layoffs and Absentee Bosses Create a Morale Crisis at Meta," *The New York Times*, 12 April 2023. https://www.nytimes.com/2023/04/12/technology/meta-layoffs-employees-management.html

2 Andy Greenberg, "Slack's and Teams' Lax App Security Raises Alarms," Wired.com, 23 September 2022. https://www.wired.com/story/slack-microsoft-teams-app-security/

3 Yunang Chen, Yue Gao, Nick Ceccio, Rahul Chatterjee, Kassem Fawaz, and Earlence Fernandes, *Experimental Security Analysis of the App Model in Business Collaboration Platforms*, University of Wisconsin-Madison, 2022. http://www.earlence.com/assets/papers/slack-teams-security22.pdf

4 Steve Zurier, "Over 90% of Organizations Had a Security Incident Linked to a Third-Party Partner in Last Year," SCMagazine.com, 23 March 2022. https://www.scmagazine.com/research-article/third-party-risk/over-90-of-organizations-had-a-security-incident-linked-to-a-third-party-partner-in-last-year

5 Joel Witts, "How Secure is Slack for Your Business?" ExpertInsights.com, 29 March 2023. https://expertinsights.com/insights/how-secure-is-slack-for-your-business/

6 Lauren Johnson, "Why Nearly 80% of Fortune 100 Companies Rely on Slack Connect to Build Their Digital HQ," Slack.com, 5 April 2022. https://slack.com/blog/transformation/fortune-100-rely-slack-connect-build-digital-hq

7 WhatsApp FAQ. Accessed April 2023. https://faq.whatsapp.com/1182985198951186

8 Peter Elkhind, Jack Gillum, and Craig Silverman, "How Facebook Undermines Privacy Protections for Its 2 Billion WhatsApp Users," ProPublica.org, 7 September 2021. https://www.propublica.org/article/how-facebook-undermines-privacy-protections-for-its-2-billion-whatsapp-users

9 Nathalie Schabio, "How WhatsApp's Privacy Policy Raises Major Concerns," Diggit, 30 January 2023. https://www.diggitmagazine.com/articles/how-whatsapps-privacy-policy-raises-major-concerns#:~:text=ProPublica%20revealed%20that%20messages%20sent,by%20Meta%20the%20umbrella%20company

10 WhatsApp Terms of Service. Accessed April 2023. https://www.whatsapp.com/legal/terms-of-service-eea

11 Irish Data Protection Commission news release, "Data Protection Commission announces decision in WhatsApp inquiry," 2 September 2021. https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-announces-decision-whatsapp-inquiry

12 ProPublica, 7 September 2021.

13 Ajay Bhatia, "The Hidden Threat of Business Collaboration Tools," SecurityMagazine.com, 4 October 2021. https://www.securitymagazine.com/blogs/14-security-blog/post/96219-the-hidden-threat-of-business-collaboration-tools

14 John Gray, "The New Tech Totalitarianism: When Companies Knows More About Us Than We Know About Ourselves," The New Statesman, 6 February 2019. https://www.newstatesman.com/culture/2019/02/the-new-tech-totalitarianism