TMI: Tech Companies' Insatiable Appetites for Data, and How Enterprises Can Avoid Over-Sharing

Sara Crifasi & Kevin DiLallo
May 2, 2019

In the past few months, we've witnessed a torrent of revelations about tech companies' collection and sharing of user information. Every link in the chain is culpable: device manufacturers, wireless carriers, app developers, social media platforms, and data brokers and analytics firms. From mobile carriers selling access to users' real-time location data,[1] to apps sharing user data (including phone numbers and IP addresses) with unaffiliated third parties, to social media platforms gathering data on not only their users' entire photo, phone, and web histories, but also on those users' (non-consenting) contacts,[2] a new data privacy scandal seems to erupt daily.

Enterprises may initially be of two minds regarding the eroded data privacy landscape. On the one hand, consumer information is more easily accessed than ever before, facilitating targeted advertising and increased consumer engagement. ("The closest Starbucks / PNC Bank / Chipotle is 0.3 miles west.") On the other hand, enterprise data is also at risk. We acknowledge that all businesses value, collect, and use data about their customers and potential customers – standard practices needed to remain competitive in dynamic industries. However, just as all businesses *collect* data, they also *provide* data. Therefore, it behooves enterprises in their capacity as data *providers* to be aware of (i) the types of data that their vendors and partners are collecting, and (ii) how those vendors and partners are making use of that data.

Employee access to company information from mobile devices and PCs -- especially without centralized control over the applications and websites those devices can access -- may expose corporate information to the same data collection, use, and sharing as users' personal information, all without the enterprise's authorization. An employee's agreement to terms of use providing access to user data does not equate to enterprise consent to the data collection.

The always-connected nature of the modern workplace means that enterprise information is at risk beyond the standard "hacking" scenario. In the current environment, trusted business partners and vendors are the very ones vacuuming up huge amounts of data about enterprise users, which they use to enhance their marketing and profitability. Inadvertent or ill-informed employee sharing of information such as location, websites visited, and purchases made should prompt enterprises to limit the data telecom and tech companies can collect from them or their employees. Access to social media from company-issued computers and mobile devices could pose additional threats to enterprise data and reputations.

What's really at risk?

Enterprises may wonder whether their sensitive information is really at risk. A peek at the terms of use and privacy policies of some leading social media platforms, device manufacturers, and app developers gives you an idea of the breadth of the data they are all collecting:

- **Facebook** collects:[3]
  - "contact information if you choose to upload, sync or import it from a device (such as an address book or call log or SMS log history)"

[1] https://motherboard.vice.com/en_us/article/nepxbz/i-gave-a-bounty-hunter-300-dollars-located-phone-microbilt-zumigo-tmobile?wpisrc=nl_technology202&wpmm=1

[2] https://techcrunch.com/2019/01/29/facebook-project-atlas/

[3] https://www.facebook.com/policy.php

- "information you allow us to receive through device settings you turn on, such as access to your GPS location, camera or photos."
- "the name of your mobile operator or ISP, language, time zone, mobile phone number, IP address, connection speed and, in some cases, information about other devices that are nearby or on your network"

- **Apple** collects the following from each user who "create[s] an Apple ID, appl[ies] for commercial credit, purchase[s] a product, download[s] a software update… connect[s] to our services…[:] name, mailing address, phone number, email address, contact preferences, device identifiers, IP address, location information and credit card information."[4]
  - Furthermore, Apple "collect[s] and store[s] details of how [a user] use[s] our services, including search queries," with the caveat that "such information will not be associated with your IP address" "except in limited instances to ensure quality of [Apple's] services over the Internet."[5]
  - Finally, and only with the user's explicit consent, Apple "collect[s] data about how you use your device and applications in order to help app developers improve their apps."[6]
- **Google** collects and utilizes user-created content including Gmail emails, photos and videos, Docs, Sheets and Slides created on Drive, contacts, calendar entries, comments on YouTube, web searches, voice and audio information, activities on third-party sites and apps that use Google's services, videos a user watches, websites a user visits, call detail (e.g., phone number called or originating received calls, call duration, etc.), and location information.[7]

Collection of data in and of itself is not novel or problematic. But it seems that companies -- by virtue of those impenetrable terms and conditions we all necessarily "click yes to agree" to when activating mobile devices, software, or apps – are sharing data about their employees (and, thus indirectly, about themselves) in ways that most individuals and even the most vigilant, regulated enterprises, have not previously foreseen. We are not suggesting that the app developers or other tech companies are doing anything nefarious or illegal, just that enterprise customers should be aware of what data they are collecting and how they are using it. Customers should also consider what they can do to protect their proprietary information from unauthorized or unintentional dissemination.

--

While the news about data disclosure has spread like wildfire because of the widespread use of consumer mobile devices, the risk is not limited to those devices. Any time an enterprise customer utilizes a SaaS service or hosted application from a laptop or desktop work station, the customer is providing data. But how much data *must* be exchanged? When contracting, determine what information the service or app provider is collecting and maintaining based on your use, what information it actually *needs* to provide the service (versus what it collects), how the provider is going to use the data, whether it will share it, and with whom, and how it stores and secures your data. Also, do you have access to the data the provider has collected about you and your users and customers? These are all legitimate and important questions to ask your provider *before* you sign the contract. We have been shocked to see that some service providers collect data from our clients and won't even share it with them! Try to limit the data you provide to the minimum needed to get full use of the service. In addition, if your enterprise has an information security policy for vendors (as most do now), don't assume the vendor will simply comply. If the vendor has agreed to comply with your policy, you can and should periodically verify its compliance through audits.

[4] https://www.apple.com/legal/privacy/en-ww/

[5] *Id.*

[6] *Id.*

[7] https://policies.google.com/privacy?hl=en

In a lawless landscape, enterprises must protect themselves

Because of the "feed the beast" nature of data monetization, unavoidable and generally non-negotiable contractual privacy waivers, and the lack of effective legal shields, enterprises must resort to self-help to protect themselves. Unlike the EU with the General Data Protection Regulation ("GDPR"), the U.S. lacks a single federal law governing the use and dissemination of personal information. Whereas the GDPR imposes significant monetary penalties for breaches (the greater of €20 million or 4% of worldwide annual revenues), breach disclosure and response requirements in the U.S. (most of which are state laws) don't pack the same punch. Many states have breach notification laws, but those laws can't put the disclosed-data toothpaste back in the tube, nor do they sufficiently compensate organizations saddled with huge clean-up costs after being harmed by a data breach. As a result, entities who collect and trade in your data operate in an environment (as least in this country) with few meaningful sanctions and ineffective, grossly insufficient enforcement of those sanctions.

--

Sources of Self-Help for Enterprises

Given the lack of legal protections in the U.S., enterprises must rely on self-help to protect their sensitive data from falling into the wrong hands, and avoid reputational and competitive harm, as well as steep remediation costs. We recommend a combination of internal and externally-directed actions.

Internal Precautions

While most large enterprises have information security policies designed to prevent unauthorized access to company systems and data, these policies tend not to address the risks discussed in this paper, namely, the use and sharing of information that was *voluntarily provided* or unwittingly consented to without enterprise awareness or prior vetting. Luckily, there are several internal actions that enterprises can take to limit that disclosure or withhold or condition that consent in the first place.

Take Full Advantage of Privacy and Security Settings. If one theme comes through clearly from reviewing telco and tech companies' websites, disclosures, and privacy policies, it is this: primary responsibility for protecting information a user does not want collected lies with the user. First, invoke all available privacy and security settings that your software, hardware, and apps offer. Second, be sure that all sensitive information is encrypted in transit from end point devices to service providers. There simply is no excuse for failing to take advantage of the prophylactic features that are handed to you, though most of us don't, at not least not fully.

Additional internal procedures are advisable if the enterprise allows employees to access corporate data, email, or apps from a mobile device, including tablets and laptops. The mobility of these devices and their connectivity via interfaces such as Wi-Fi, Bluetooth, and commercial cellular services, plus the blending of work-related and personal use on a single device, makes them inherently more vulnerable to over-sharing of data that could be misused or shared with unknown third parties.

Mobile Device Management. Installing mobile device management ("MDM") software on employees' mobile devices allows enterprises to protect company data stored on the device and control employee access to unvetted apps and high-risk sites, even if the enterprise has a complete or partial Bring-Your-Own-Device ("BYOD") environment. MDM software commonly includes password protection, two-factor authentication, and data encryption, plus the abilities to remotely wipe data and dictate which apps are permitted (whitelisting) and which are prohibited (blacklisting). If you deploy MDM software, you should secure employee consent to manage work-related content on the mobile device, coupled with a waiver of claims by each user for any over-deletion that may remove personal content that was commingled with work-related content.

App-control capabilities are key. Preventing employees from downloading and using apps that could disclose or access sensitive information is a good starting point, but encrypting data stored on, and transmitted from, the device provides an important backstop. Many enterprises have their own app stores where they make whitelisted apps available to employees. Only apps available through the enterprise app store may be downloaded to a device that has access to enterprise systems. One caveat about MDM software: it is unable to override certain native apps on the iPhone and Android devices, so if those are the source of a problem, you may have to rely on an employee policy to curb risky behavior.

Employee Training and Policies. Because your employees are the last line of defense before your information is shared with others, it is critical to sensitize them to the risks of such dissemination and instill a shared sense of responsibility for guarding against those risks. Every company should have a written IT policy detailing, as applicable, whether MDM software is required, which websites and apps are permitted and which are prohibited, how work-related communications (whether oral or in writing) on mobile devices should and should not be made, and which permissions (e.g., location sharing) and features (e.g., Bluetooth, Wi-Fi) should be turned off. Of particular and recent concern are features allowing employees to record conversations and conference calls and to archive written communications, social media posts, and web searches.

Remember that laptops are mobile devices and share many of the same vulnerabilities as smartphones and tablets. Remind employees of this policy on a regular basis and have them accept the terms in writing annually. Of course, managing employee devices is easier with enterprise-provided devices and service plans. BYOD programs by their nature have a greater risk of commingling personal and work-related data and, accordingly, disseminating sensitive data. You might even consider subsidizing a cloud storage account for employees' personal data and photos and requiring weekly or bi-weekly back-ups to reduce the risk of losing cherished personal information during a remote memory wipe.

External Precautions

Contract Language. While enterprises may not have contractual privity with all the entities in the chain of communications between their users, customers, partners, and suppliers, they should insist on data security language in service agreements with the entities with whom they do have privity, including their wireless carriers and SaaS providers. At a minimum, these agreements should prohibit service providers from monitoring or accessing the content of communications sent, received, stored, or processed using their services, regardless of any click-through terms or software licenses. In light of recent reports of carriers' rampant location information brokering, mobile service agreements should also include language prohibiting carriers and their associated third parties from disclosing device location information absent just-in-time explicit user consent (except, or course, in an emergency or where required by law).

Unfortunately, this approach does not work with the major wireless OS developers and device manufacturers, including Apple, Google, and Samsung; almost all enterprises buy their products through a VAR, most commonly a wireless service provider, so there is no direct contractual privity between the enterprise customer and the device manufacturers/OS licensors, and virtually no leverage an individual enterprise can wield in negotiations with these entities.

If you contract for a customized, enterprise-specific app, whether for internal management or external customer purposes, carefully consider the data that the app developer needs to collect to fully realize the purposes of the app, including how that data will be used for such purposes, and document limitations on all other data collection in your agreement with the app developer. Be sure your negotiated agreement takes precedence over any click-through or other extra-contractual terms. Ensure that the app developer is not sharing the data you input (or it otherwise collects, e.g., with cookies) with any entity or for any purpose you haven't explicitly approved. For example, your internal productivity and communications app may not have any need for location services, an easily-memorialized restriction. If the app must collect any of the enterprise's data to operate effectively, the agreement should require that the data be anonymized and aggregated.

Strength in Numbers. To effect change with a broader scope (i.e., beyond your contract alone), consider coordinating with others in your industry or with similar objectives and acting through a trade association or similar organization to advocate for greater transparency around data collection and usage. Such coordinated efforts can bring benefits such as enhanced leverage, portrayal of the issue as an industry-wide concern, spreading the cost of advocacy, and making for good public relations.

Obviously, there is tension between every business's need to collect third parties' data to remain competitive and its desire to limit the amount of its own data that others collect and use. This tension means that a legislative or regulatory privacy fix is unlikely, as most businesses are on both sides of the debate. But greater transparency and control over one's own data are goals that all responsible businesses should support, if for no other reason than achievement of those goals could obviate the need for heavy-handed regulation along the lines of the GDPR. And because all legitimate players would benefit from voluntary efforts designed to facilitate data collection while heightening awareness of, and participation in, the process by those from whom the data is collected. Not only would businesses benefit from such reforms, their individual employees and customers would as well.

--

The telcos, app developers, and other data aggregators increasingly echo Sir Arthur Conan Doyle's Sherlock Holmes – "*Data! data! data! I can't make bricks without clay."* But just because they're continuously building does not mean that your enterprise must supply the raw materials.

If you would like more information about data collection or measures you can take to limit the data your vendors and partners collect, or if you would just like to brainstorm these issues, call or email Kevin DiLallo (kdilallo@lb3law.com; 202-857-2560) or Sara Crifasi (scrifasi@lb3law.com; 202-857-2561).