Ethical Enterprise

Understanding the Software License Terms that Impact your Online Privacy

IEP Equity White Paper 20-04-01

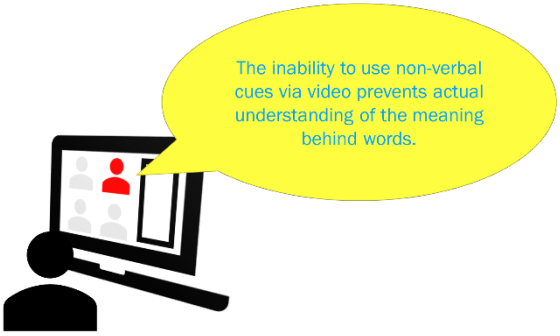
Chris Draper, Ph.D., P.E., IEP Equity and Trokt

Angie Raymond, J.D., L.L.M, Indiana University

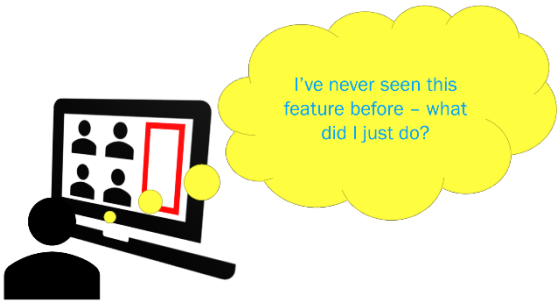
Video conferencing technology's overnight change from a "nice to have" feature to a "mission critical" collaboration tool has shone a light on previously underappreciated data security issues. Zoom, which went from an all-time high of 10 million users per day to a daily average in March of 200 million users per day nearly overnight,[i] has borne the brunt of this scrutiny. Articles like those published in the New York Times have been quick to highlight bugs, scale-up glitches, or investigations.[ii] Yet technology experts have rightly pointed out that the majority of these data breaches are not "hacks" of the Zoom, Microsoft, Google, GoToMeeting, WebEx, Eyeson, or any other provider platform. They are user mistakes.[iii] No matter the platform, t***he operator remains an organization's biggest security risk.***

Operational data security risk for collaboration platforms derives from two primary sources:

1. An inability to effectively communicate using the platform, and

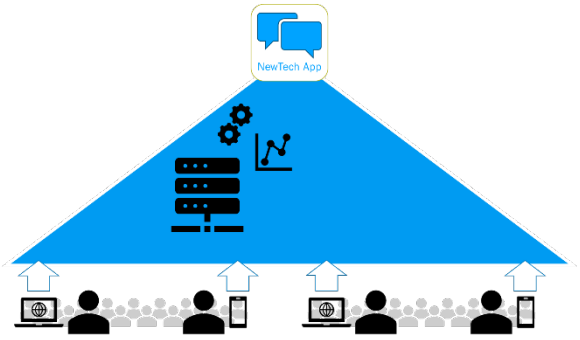


2. An inability to use the platform effectively.



The myriad of data security issues that get the most publicity – from "Zoombombing" to illegal recording to archive misdirection – are typically human errors that can occur in any of the current collaboration platforms. Some of these errors are magnified by platform user interface (UI) or user experience (UX) design choices that can only be mitigated with familiarity and competency-based training programs.[iv] Yet systemic user errors – and the data breaches they regularly cause – are too often the result of unintended system configurations. Reducing the risk from these types of data breaches requires decision owners to understand a platform's general architecture, how the platform will integrate within the user's work processes, and which functions must be contractually modified during an enterprise installation.

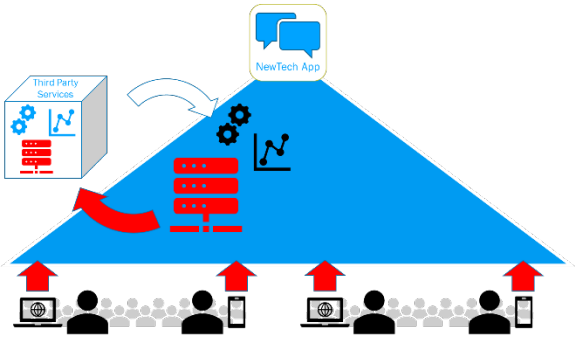
Modern Software is Modular

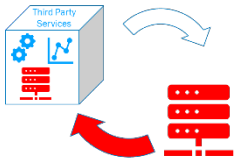


Software platforms use data gathered from a broad range of devices to complete various processing and analytical functions that perform the actions requested by a user. For example, the NewTech App on a user's phone may allow the user to dictate a message, a process will turn the spoken words into text, an analytical function will search for ineffective language, and the NewTech App will provide the user with suggestions for improving message effectiveness.

Many people may be familiar with software that was built all by one company, installed on a computer from a disk, and effectively operated in its own silo. This is not how software is built anymore. Any single software platform will contain any number of software languages, language libraries, or reused code snippets. For example, the language that tells an internet browser *how to display* a website will almost always be different than the language used to tell that website *what to display*. Yet many platforms that serve different purposes will still perform identical functions. For example, most platforms not only use the same process for logging in, many use the exact same single sign on (SSO) code and connectivity relied upon by hundreds to thousands of other websites (e.g. "Sign in with Google" options).

Many modern software platforms depend on third-party systems to perform a wide range of critical tasks. Any third-party system integrated into a user selected NewTech App will take the data it is sent, store at least what it needs to operate, run the necessary processes or functions, and send back the requested output. For a platform that integrates third-party systems to operate, user data must be shared with that third-party. In nearly every software license agreement is a typically broad section defining what any NewTech App shares to a third-party software and for what purpose.





Microsoft collects data from you, through our interactions with you and through our products for a variety of purposes described below, including to operate effectively and provide you with the best experiences with our products. You provide some of this data directly, such as when you create a Microsoft account, administer your organization's licensing account, submit a search query to Bing, register for a Microsoft event, speak a voice command to Cortana, upload a document to OneDrive, purchase an MSDN subscription, sign up for Office 365, or contact us for support. We get some of it by collecting data about your interactions, use, and experience with our products and communications.

We rely on a variety of legal reasons and permissions (sometimes called "legal bases") to process data, including with your consent, a balancing of legitimate interests, necessity to enter into and perform contracts, and compliance with legal obligations, for a variety of purposes described below

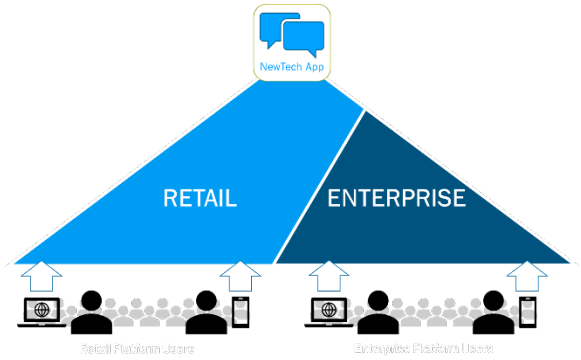
Retail users of a software will have little to no authority over what is shared, with whom it is shared, and for what purpose it is shared. In some cases, the amount and use of data sharing risks data security. For example, platform developers who integrate Facebook functions or features have often needed to accept third-party permissions and controls like those that

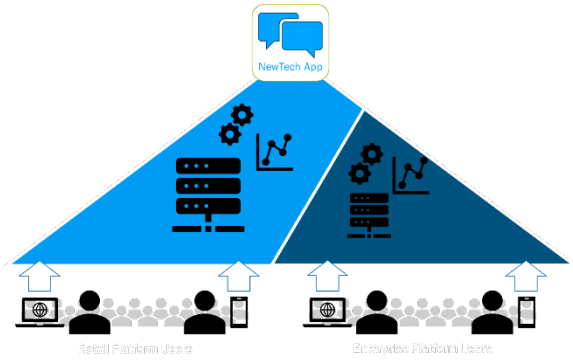
led to the Cambridge Analytica scandal.[v] These kinds of integrations are often "take it or leave it" options: if a NewTech App user does not want to share data with a specific third-party, then the NewTech App cannot be used. To exert greater control over what is shared to a third party, many platforms offer enterprise versions.

Enterprise Software

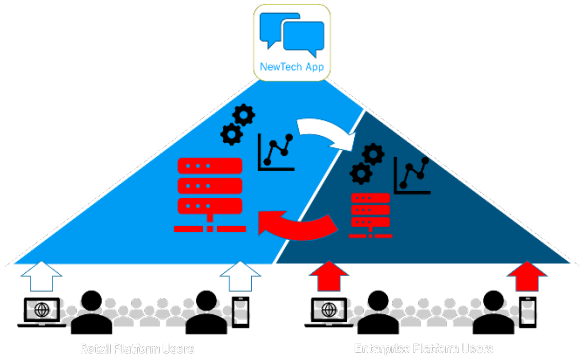
Many organizations want all their members to use particular software platforms to complete specific business processes in an identical manner. For example, an organization may want to allow its customer to speak with customer service through a NewTech App. However, the organization wants to ensure every customer has the same experience using the NewTech App no matter which customer service representative receives the initial message. Therefore, the organization could install an enterprise version of the NewTech App that would automatically log, assign, and track customer engagement through the NewTech App in an identical manner every time.

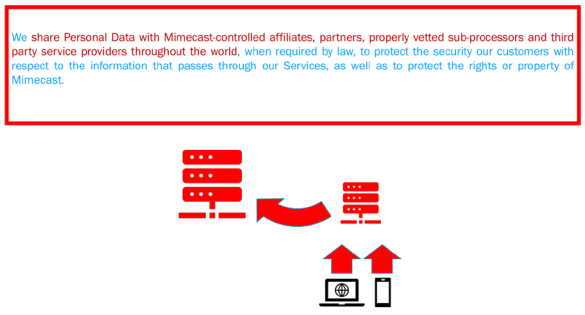
There are many ways to create an "enterprise" installation of a modern technology application. When cloud-based applications do this by creating a supposed silo between systems, it is important to ensure the level of separation between the core (i.e. Retail) product and the Enterprise offering.





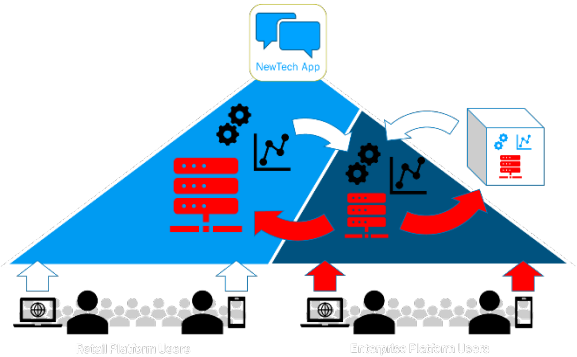
These types of systems may require processes depend upon data managed by the core system. For example, processes dependent on artificial intelligence (AI) may be unable to maintain system performance while being functionally siloed. In these instances, data will be shared between the enterprise and core system similarly to the retail third-party relationship.

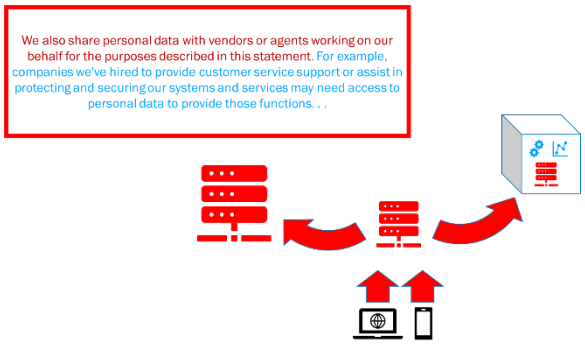




Enterprise customers and users must examine how and to what extent an enterprise system is separated from the core platform. Significant flexibility may exist with respect to what types and quantities of unmodified data is shared, or what type of anonymization is performed if data sharing cannot be prevented.

Similarly, enterprise customers or users must also be conscious of the data sharing, storage, and usage relationships between any additional third-party platforms that are connected at the direction of the Enterprise customer. For example, a NewTech App may be deployed by a company that also uses a CRM to track the entire sales and contracting process means data could not only be stored out on an additional third-party platform, products from third-party processes may produce new data that could be shared back into the core system.

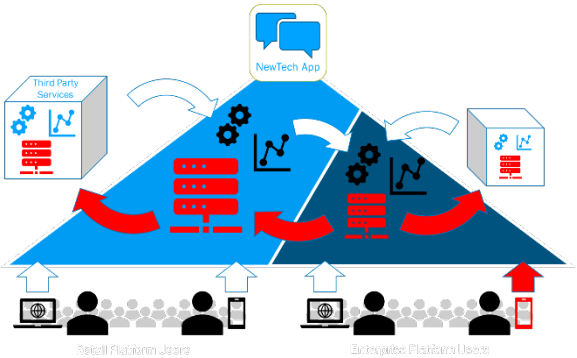


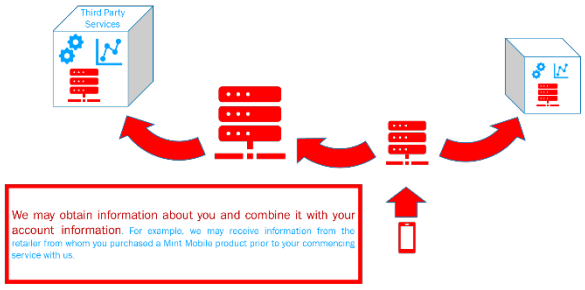


Making Ethical Choices

It is extremely important to understand that intentional misuse of data like that seen in the Facebook/Cambridge Analytica scandal is extremely rare. Yet our technology decisions must account for the fact that keeping large data stores which continually appreciate in value pose significant risks, risks that we are ethically bound to mitigate.

For example, if an employee of a NewTech App enterprise customer connects via mobile phone while on the organization's Wi-Fi network, the enterprise platform may likely be gathering phone location data in order to optimize service performance. This data could easily be stored at the enterprise, core, and multiple third-party levels, similar to how cell networks used CarrierIQ for network optimization. After it became know that CarrierIQ was keystroke logging every action being taken by the majority of network connected tablets and cell phones across American, the result was a $9B class action settlement.[vi]

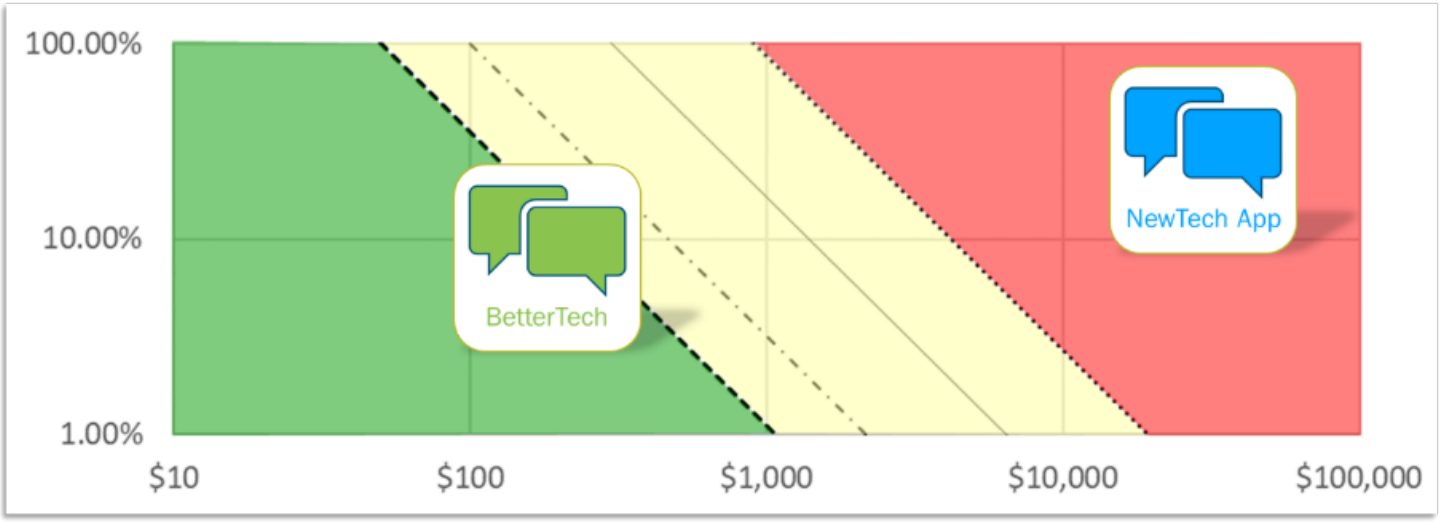




The CarrierIQ settlement cost is an outlier in the world or data security, yet data misuse carries access to significant consequences. While violations of the Federal Privacy Act carry statutory penalties of $5,000 per violation, modern collaboration platforms could pose greater financial risks. For example, school privacy normally falls under the Family

Education Rights and Privacy Act (FERPA). However, some enterprise software providers may be pushing consent responsibility for Children's Online Privacy Protection Act (COPPA) onto unknowing schools, opening up civil penalties of $41,484 per violation.[vii] Worse yet, misconfigurations of multi-platform systems could result in recordings or transmissions that may be felony violations of Federal Communication Council (FCC) regulations.

It should be extremely unlikely that a retail or enterprise collaboration platform will result in these types of consequences without a user acting in bad faith. Yet operational data breach rates for widely used collaboration systems – email, text message, cloud docs – routinely demonstrate that these systems pose inappropriate levels of risk.[viii] Plotting the risk posed by these tools against the Draper Catastrophe Value Curve (CVC) demonstrates that an economically accessible alternative should be employed.[ix]



From a data security perspective, the American Bar Association *Model Standards Rule 1.6: Confidentiality of Information* comments[x] state that ***selecting or maintaining a higher risk platform despite economic access to a lower risk alternative is unethical***.

[i] https://blog.zoom.us/wordpress/2020/04/01/a-message-to-our-users/
[ii] https://nyti.ms/3auOg1H
[iii] https://agileattorney.com/zoom_is_safe_for_lawyers
[iv] Draper, C.H., *Online Dispute Resolution Data Security*, Online Dispute Resolution: Theory and Practice [awaiting publication]
[v] https://www.vox.com/2018/3/20/17138756/facebook-data-breach-cambridge-analytica-explained
[vi] https://topclassactions.com/lawsuit-settlements/closed-settlements/332122-smartphone-privacy-class-action-lawsuit-settlement/
[vii] https://www.edweek.org/ew/issues/childrens-online-privacy-protection-act-coppa/index.html
[viii] Draper, C.H. and Raymond, A.H., Ethical Technology Risk: How to identify what is reasonable data protection for ODR, 12 Int'l J. Dispute Res. (2019)
[ix] Draper, C.H., & Raymond, A.H., "Building a Risk Model for Data Incidents: A Guide to Assist Businesses in Making Ethical Data Decisions," Business Horizons, 2019, ISSN: 0007-6813, https://doi.org/10.1016/j.bushor.2019.04.005. (accessed July 7, 2019)
[x] https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_6_confidentiality_of_information/