Rubric for Video Conferencing Tools

The below rubric is perhaps more detailed than most teachers may need, but it may be useful to schools or systems, IT departments, or educational leaders to guide discussions of possible tools. There are other tools beyond those listed, but these are the most commonly used within education. For different readers and groups each category may have different significance. For example, where cost is a prohibitive factor, free tools will have primacy, it is important to be aware of what limitations each 'free' tool has, as they may not be appropriate depending on the size of your class or organisation. Where teacher aptitude with technology is low, the interface and features may be important. Data use and encryption should be important considerations for both the protection of teacher and student data as well as protecting both from outsiders accessing the software or the meetings therein. Of greatest practical importance is whether the tool is platform or stand alone, as a platform-centric tool will work best with the coterie of other tools associated with it. For this reason, the Educational Technology space is often depicted as a duopoly of Microsoft and Google, with Apple and Adobe as smaller also-rans. However, in the videoconferencing space Zoom stands head and shoulders above its competitors due to it being stand alone, intuitive and inexpensive.

	Companies privacy score	Type of data collected	Data Collection and it's use	Cost	Encryption	Teacher & Student-friendly features	Intuitive Interface	Platform or stand alone	Source-code
Jitsi	N/A	Basics for use	None	Free	Hop-by-Hop (E2EE available, but isn't the default)	Medium	Yes	Stand alone	Open
Microsoft Teams	4.5/10	Basics for use + Improving products	Limited	Free OR $12.50 / month	In-transit and at rest	Medium	Yes	Microsoft Office 365 (Platform)	Proprietary
Webex (Cisco)	N/A	Basics for use + Improving products	Limited	Free	In-transit and at rest (E2EE available, but isn't the default)	High	No	Stand alone	Proprietary
Adobe Connect	N/A	Basics for use	Limited	$50 / month	None	Medium	Yes	Stand alone	Proprietary
Facetime (Apple)	6.5/10	Basics for use + Improving products	Limited	Free	E2EE	Low	Yes	iOS (Platform)	Proprietary

Skype for Business	4.5/10	Basics for use + Improving products	Limited	Free	Transport Layer Security (TLS) + AES 256-bit encryption	Low	Yes	Stand alone	Proprietary
Zoom	3.6/10	Basics for use + Facebook details + IP address and device type	Concerning	$20 / month	Transport Layer Security (TLS) + AES 256-bit encryption	Medium	Yes	Stand alone	Proprietary
House Party	0.7/10	Everything available	Concerning	Free	None	Low	Yes	Stand alone	Proprietary
Google Meet	4.8/10	Basics for use + Improving products	Concerning	Free / $12 a month	In-Transit	High	Yes	G-Suite	Proprietary
Google Hangout	4.8/10	Basics for use + Improving products	Concerning	Free / $12 a month	In-Transit	Medium	Yes	G-Suite	Proprietary

Companies privacy score: This information is provided courtesy of Privacy Spy, this rating is a very useful way to get a broad overview of each company's overall privacy record. Note: it is not specific to the tool, but rather the organisation that provides the tool, its rubric makes use of 'Transparency, Handling and Collection' through the lens of privacy. The focus of these ratings is a close analysis of the privacy policy and therefore transparency and user control and access to personal data is held at a premium.

Type of data collected: 'Basics for use' denotes those things that would be expected, namely email addresses, usernames and other details automatically entered into the software, as well as record of calls and other users you have connected with. 'Improving products' essentially means recording usage statistics, activity peaks, function use and so on, with an eye to improving the product by plotting how often or how frequently features are being used. An easy analogy to understand this concept is a phone exchange, it will collect who calls whom and at what time. For the 'improving products' type features, this would mean, within the analogy, that the phone exchange might hire additional operators to direct calls during peak periods. As this rather inert analogy suggests, data collection by itself is not necessarily problematic but must be considered in light of the next section in regard to the way that it is then used, and the concept of trust is of the utmost importance in this interaction.

Data Collection and its use: The amount of data collected and the purposes that it is collected for are both important here, so an exploration of each example and these factors intertwining will be elucidated. For House Party, the data collection is not clearly defined, or capped, neither is the use of this data within their privacy policy, as can be seen from the tools parent company (Epic Games) privacy score. Zoom's data collection is concerning because it doesn't protect the data, can be easily accessed by outsiders and communicates the information it does collect to third parties, including Facebook, even

when this tool is not connected to the platforms use. Lastly, Google makes use of this data, which by itself may seem inert, within a much broader detailed record of its users' character, interests and habits to more effectively target users with advertisements. For these reasons, the amount of data collected, the way that this data is then used, or shared with third parties are all important to consider when choosing a tool. This statement is especially true if you are a teacher, using these tools with your students, for whom their engagement with your class may constitute a form of surveillance and data-gathering that is then combined with their 'out-of-school' lives to improve the algorithmic delivery of advertising to them.

Cost: This element is in some instances more complex that has been summarised here. This is especially true for Google and Microsoft products which sit within a broader enterprise solution, Microsoft Office 365 and Google for Education suite, which opens up a range of possibilities for webhosting, hardware and software packages that will range in price. Similarly, Adobe Connect sits within a broader suite of tools but does not require them as part of a platform choice. So, it's important to consider not only a video conferencing solution, but also the broader costs, including teacher professional development, that is invisibly tied to a platform adoption or a shift to a new platform, and to a lesser extent a new tool.

Encryption: Without trying to overcomplicate things, encryption is the process of coding information that can only be 'decoded' by another 'key', due to a basic tenet of mathematics this system can be 'cracked' without a key, but this process takes decades. It is easiest to think of our telephone exchange analogy again, each video call has at least two interlocutors and the exchange (server) in-between. End-to-End Encryption (E2EE) is the gold standard and means that at all points between these three (or more) locations, the data (audio and video feed) is encrypted. Other types of encryption include 'at rest' which only encrypts data whilst it sits idle on servers, 'in transit' which encrypts whilst the data is moving between servers and finally a blend of the two options which is called 'hop-to-hop'. Some services do not encrypt data at all, which has benefits not only to the company, but also anyone who has designs on your information. Transport Level Security (TLS), occurs in transit and is commonly used for email and web browsers and is displayed by the lock image next to browser URLs, simply put, this method means that data is not encrypted on servers. It is encrypted, but only in transit, which means, in plain terms, that the companies have access to the audio and video files of its meetings whilst they are on their servers. Encryption is of premiere importance when dealing with information that is sensitive, since school uses of videoconferencing involve minors and a range of sensitive information its security is paramount. In plain terms, End-to-end encryption is the gold standard and means that the company providing the service cannot access your information. Any other form of encryption shows effort but allows in various vulnerabilities that are able to be exploited by the company itself or nefarious outsiders.

Teacher & Student-friendly features: This section is subjective and experiential, teachers require a slightly different range of features within videoconferencing software, as provided within the checklist. Unfortunately, often educators are left to make do with enterprise tools and software that are either slow to respond, or never respond to teachers requests for the specific features they need. Within videoconferencing tools that are ideal would include features such as: Breakout rooms for collaboration, waiting rooms and / or password protection to keep out interlopers, 'Mute All' options, having the ability to make one user (the teacher) have greater control over the interface, Screensharing, a tiled view to allow for multiple speakers (such as a class of students), native polling and 'hands up' functions are all highly important. Rather than list these elements, I've provided my experience of using each tool into 'High' (Google Meet and Cisco Webex), 'Medium' (Jitsi, Teams, Zoom, Google Hangout) and 'Low' (Facetime, Skype for Business and House Party)

categories, but if you're setting requires different features than those here, it's worthy of further investigation. As technology is a tool, in some cases, the choice can allow for a wider range of pedagogies or conversely restrict them, so these features are important.

Intuitive Interface: Coverage of User Interface (UI) and user experience (UX) are mostly concerned with ease of use, intuitiveness and accessibility, these concepts hold even greater challenge and import in the realm of education. Choices around platform should include not only a consideration of how intuitive the software is for a new user, but also consider what prior experience your student body has with technology. Students may have previous experience with similar platforms that would allow greater ease of integration and thus, hopefully, more ease engaging with set content.

Platform or stand alone: As mentioned above, whether the tool selected exists within a platform of broader products is pertinent. Using Microsoft Teams in combination with Google document applications is possible, but unfortunately not ideal, as the format and skills, are not always transferrable. Therefore, a stand-alone product may be more suitable if your focus is on students achieving success with a limited number of tools. The negative effects of technology platforms (Bartlett, 2018; Srnicek, 2017) and their further 'siloing' of the teaching profession along technological lines, in this realm holds a positive effect in the way that it limits the technological knowledge required of students if they remain on one platform. If the platform option is selected, the importance of selecting trust-worthy tools that are not using the platform, 'walled garden' approach to more effectively collect extensive data on the students under your care.

Source-code: Within Education International there is a movement to greater freedom of information, especially in regard to the use of creative commons licencing for intellectual property produced by teachers and fair use of existing materials for educational purposes. Though this may not seem like a pressing concern in any adoption of a new technology, considering open-source software is something not to be overlooked for the comparative safety implicit within this type of code. The open sharing of ideas, in this case code, is also a useful metric for trust, because it doesn't easily lend itself to being monetised, as in the case of the platform Jitsi above.

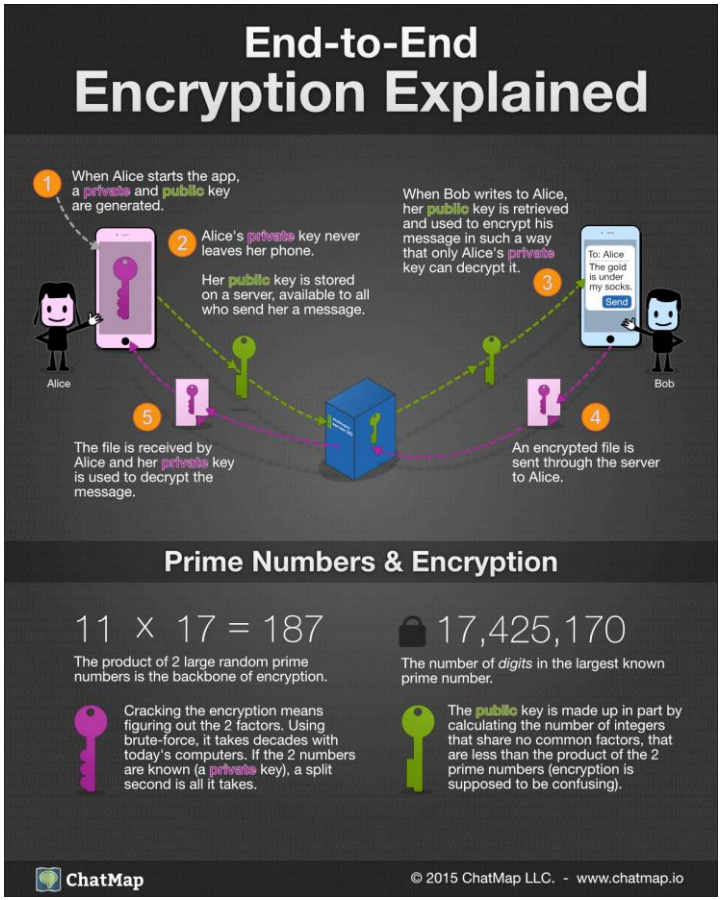
References

Bartlett, J. (2018) The people vs tech: How the internet is killing democracy (and how we save it). Random House.

Srnicek, N. (2017) Platform capitalism. John Wiley & Sons.

Further reading

A quick guide to encrypted messaging:



Source: https://www.poweradmin.com/blog/a-quick-guide-to-encrypted-messaging/

Video conferencing Webex, Microsoft and Google platforms compared in terms of data policies and practices:

Videoconferencing Services

A comparative analysis of privacy policies

Top 10 Criteria	Webex from Cisco	Meet, Duo, and Hangouts from Google	Skype and Teams from Microsoft
How might my data be leaked?	Hosts and participants can potentially record calls. The recordings could be shared without the knowledge or consent of participants.		
What do VCs directly collect from me?	Identifies data collection in Privacy Policy but may ask for additional information via "just-in-time" notice.	Collects identifiers about user devices that can be used to identify a person.	Privacy Policy presents detailed info on data collection. Privacy Policy references VCs.
Do VCs collect info about me from other companies?	All VCs include language in privacy policies that suggest or imply they collect data about users from other companies. The policies lack detail on data sources and elements they collect.		
How do third party organizations share or use my data?	All Privacy Policies describe when third parties can access data. For instance, sharing a file on VCs means everyone can access it. They do not clearly articulate the types of data sharing. Some types of sharing could support behavioral profiling.		
How do VCs differ by usage (Ex. school vs. work)?	Services vary by customer: individuals, schools, businesses. Administrators of service will have rights to track users. Due to having different rules within different organizations, participants might not be aware of who controls a meeting, and who might be able to access it after the fact.		
Will my data ever be deleted or retained as noted in the privacy policy?	Policy defines windows of up to seven years before all data gets deleted.	Policy defines different rules for data retention but the rules may not be not clearly articulated for end users.	Policy references data deletion but states that actual retention periods can vary significantly.
What are the differences between data collected from VC hosts vs. participants?	Main privacy policy does not address this issue; a Webex specific addendum highlights additional information collected from hosts.	Privacy policy does not address this issue.	Privacy policy highlights VCs but no distinctions between data collected from participants vs. hosts.
How is my information used for product improvement?	Privacy policy claims broad rights over how Cisco can use personal information.	Privacy policy explicitly defines Google's right to use the data they collect to develop new products.	Privacy policy states Microsoft uses data to improve existing products and add new features.
How might my data be sold or shared as part of a transaction?	No mention of a need to notify or inform end users if a transaction occurs.	Privacy policy defines data as an asset that can be transferred and promises to provide notice that data will be transferred.	Privacy policy defines data as an asset that can be transferred as part of a sale.
Will the VC have access to my data for machine learning, AI Analysis or human review?	Policy mentions, but does not place consistent limits on, data use for ML or AI, and/or human review.	Policy mentions Google reserves the right to access data for AI analysis and automated review.	Policy describes how Microsoft uses "manual methods" to review data that has been processed and/or analyzed via AI.

VCs = Videoconferencing Service/s
Privacy Policy = Terms of Service

Last edited: April 30, 2020

CR Consumer Reports | Digital Lab

Summary results comparing the privacy policies of Webex, Meet, and Skype

Source: Consumer Reports, available from: https://medium.com/cr-digital-lab/skype-meet-webex-videoconference-privacy-845bc8360fd3

use

Useful websites for further information

Google, Microsoft, WebEx comparison – Consumer Reports

https://www.consumerreports.org/video-conferencing-services/videoconferencing-privacy-issues-google-microsoft-webex/

Cisco Webex encryption

https://blog.webex.com/video-conferencing/four-key-security-features-of-cisco-webex/

Comparing Adobe Connect to Skype for business

https://www.trustradius.com/compare-products/adobe-connect-vs-skype-for-business

Cisco Webex privacy

https://trustportal.cisco.com/c/dam/r/ctp/docs/privacydatasheet/collaboration/cisco-webex-meetings-privacy-data-sheet.pdf

Adobe Connect Privacy

https://helpx.adobe.com/adobe-connect/adobe-connect-gdpr.html

Jitsi security

https://jitsi.org/security/

https://www.makeuseof.com/tag/jitsi-secure-zoom/#:~:text=Jitsi%20uses%20hop%2Dby%2Dhop,it%20to%20the%20video%20participants.

Zoom encryption

https://theintercept.com/2020/03/31/zoom-meeting-encryption/

Apple Data use

https://www.zdnet.com/article/apple-data-collection-stored-request/

Zoom Privacy

https://securityboulevard.com/2020/03/using-zoom-here-are-the-privacy-issues-you-need-to-be-aware-of/

Zoom lack of encryption

https://www.theverge.com/2020/6/3/21279355/zoom-end-encryption-calls-fbi-police-free-users

Zoom encryption (TLS)

https://zoom.us/docs/doc/Zoom-Security-White-Paper.pdf

Video Conferencing comparisons

https://vpnoverview.com/internet-safety/business/video-conferencing-software/

Microsoft Security Guide

https://docs.microsoft.com/en-us/microsoftteams/teams-security-guide