Privacy and Security by Design In a Messaging Product for Kids

Liz Allen, *Clever Inc.* Nikhil Bhatia, *Clever Inc.* Chloe Caelynn, *Clever Inc.*
Spencer Caton, *Clever Inc.* Ulziibayar Otgonbaatar, *Clever Inc.* Sriram Seshadri, *Clever Inc.*

Abstract

Designing and engineering a messaging system that is used by 6.8 million students and half a million teachers in K-12 schools is no easy feat. While the typical threats against online systems from unauthorized and unauthenticated access to sensitive information remain, the school environment compounds privacy challenges as additional entities such as guardians, co-teachers, and service providers all play a role.

The challenges arise in implementing a strict security mechanism to ensure sensitive data and messages between students and teachers are encrypted and protected, while maintaining that only authorized personnel, whether teachers, guardians, or co-teachers, can access messages. In this paper, we discuss privacy challenges we faced while creating the Clever Messaging [1] product, and the security, privacy, and technical aspects of three key product features to address those challenges.

1. Privacy in a messaging system

As the pandemic hit, Clever wanted to build a tool to ease communication between guardians, students, and teachers through a messaging feature. Messaging introduced a new type of data Clever had not handled before, User Generated Content (UGC). UGC requires additional controls to ensure privacy for our students and teachers and to comply with legal obligations. As we started building the product, we engaged our legal team to think through the various privacy implications and verify the correct technical and disclosure requirements were in place. Both state and the federal governments have laws to protect children. Clever was already compliant with all relevant state and federal laws with respect to its main rostering product, but the addition of UGC triggered additional obligations. This included updating the Terms of Service to include a “User Contributions” section[6] and understanding the obligations surroundingCchild Sexual Abuse Material (CSAM) [9] and grooming. While CSAM is a tough topic [10], it is legally and morally imperative to understand how such harms occur and how to detect and mitigate such harm within the product. Clever also established an internal UGC policy to establish and then communicate how to handle UGC internally. This included permissioning and escalation, as well as response in the event of abuse.

After understanding the legal landscape, Clever decided the first control we wanted to build into the product was an authentication authorization model to ensure that the teacher was in control of the messaging channels, as highlighted in Figure 1. To do this, we restricted communication between a teacher and a student or guardian unless the teacher had been explicitly connected to the student by the district. By requiring that the teacher be connected to the students and the guardians within the teacher roster, we ensured that all channels were reset and decommissioned at the end of the school year when students enter a new teacher’s class.

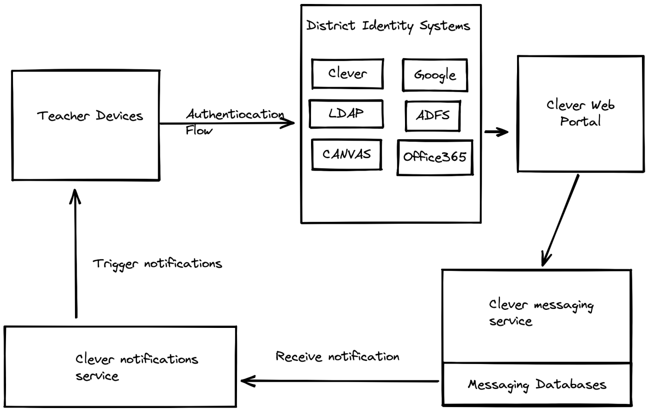

Figure 1: Overview of how a teacher logs in to use Clever Messaging.

Additionally, we built restrictive permissioning to ensure that Clever’s internal support tools did not provide access to UGC by Clever team members. As the product evolved, we introduced the ability for district administrators to audit these messages and for teachers to hide messages in the channel. We added features to detect troublesome language and provided a nudge to the user to revise before posting messages.

Because of the sensitivity of the content (these messages would not just be about math homework but could also sometimes reveal things like a child struggling with mental health or behavior), we launched our first iteration of the messaging feature in this limited manner. We wanted to make sure students were protected first, and thus we scoped the product to be just messaging between teachers and students or guardians, for the students specifically rostered to that teacher. We also launched the product to a small number of districts to troubleshoot and address any issues we might discover. This multi-phased approach ensured we had adequate security and privacy in place within the product.

2. Key Features

We will examine three key features built during the first iteration of Clever Messaging: section-based announcements, attachments, and translations.

2.1. Section-based Announcements

One of the most popular feature requests from teachers is messaging multiple students at once. Thus, in Clever Messaging, the teachers, and only the teachers, can create announcements to the same groups and can make as many announcements as they need. If a student replies to the announcement, the teacher can respond in a one-on-one manner.

When students receive messages from their teachers, it is of the utmost importance to have it be genuine and authentic. Unauthorized individuals accessing teacher accounts and creating an announcement to reach many students could pose real harm, including CSAM and grooming. Likewise, we also know that on the receiving side of things, it is vital that students and guardians are properly scoped to the school section, and only those people receive the announcement from the teacher.

The application ensures that only the teachers that are assigned to sections via the school's Student Information System (SIS), or a district data repository, can create an announcement. as shown in Figure 2. The announcement is scoped at the time of creation to only be visible to those members of the roster (students and their guardians), and any further additions and deletions from section information are reflected by the data model of the messaging system.

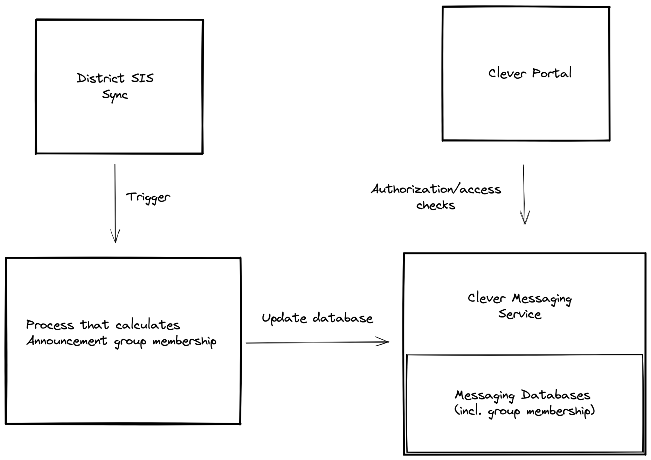
District SIS Sync
Clever Portal
Trigger
Authorization/access checks
Process that calculates Announcement group membership
Update database
Clever Messaging Service
Messaging Databases (incl. group membership)

Figure 2: With each district SIS data sync, announcement group memberships are updated according to the new rostering data.

Each modification to a SIS, like a removal of a student from a class section, must be processed immediately and reflected within the messaging product to ensure that the principle of least privilege is ensured every single step. We built Clever from the beginning with an automatic SIS syncing feature [7], thus, as soon as data is synced to Clever, the rostering change appears within the district accounts. This means that a teacher would lose the ability to use Clever messages to a student that switched sections.

2.2. Messaging Attachments

A related but distinct feature of the messaging system is the ability for teachers to send images and other files, such as homework. The storage and retrieval of such files becomes pivotal as files can include very sensitive information only scoped for a few individuals. Additionally, the nature of the usage of the messaging product makes it a prime target to spread malicious files. In 2020 alone, the cybersecurity posture of K-12 institutions saw a drastic increase in terms of cyber incidents, with ransomware attacks being a significant contributor, 12% of total reported 408 incidents [2]. Such concerns factor directly into the threat model of the file attachments in the messaging product.

To address this concern, we ensure that every time a teacher or student uploads a file via messages, the system asynchronously detects virus and malware in real-time on demand, as shown in Figure 3. A file that is identified as malicious is automatically quarantined and removed altogether, while alerting relevant engineers of the actions taken to help monitor and detect large scale targeted activities.

Additionally, we know that attachments can contain CSAM and other high risk materials, so we built the capacity for district administrators to audit messages and attachments.

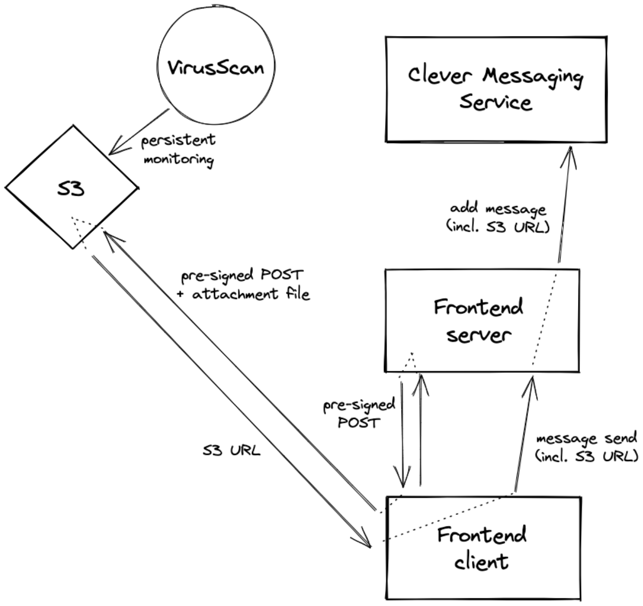

Figure 3: Attachment files are uploaded directly to the AWS S3 bucket via pre-signed HTTP POST request and are continuously monitored by VirusScan[8].

2.4. Translations

Language barriers between teachers and parents are increasingly common and detrimental to students' learning. Over 22% of families in the U.S. don't primarily speak English at home [3]. In a survey conducted by ClassDojo, 75% of teachers reported that non-English speaking parents were less engaged in classroom activities. In order to meet the needs of teachers and guardians, Clever implemented our in-product message translations.

As the first of designing in-product translations, we identified a data subprocessor that could power auto-translation of messages into multiple languages at scale with the heightened data security constraints imposed on student data. Legally, the data that is sent for translation must remain within the U.S. territory and, as the user generated messages as fall under data residency clause of Children's Online Privacy Protection Act (COPPA) [4].

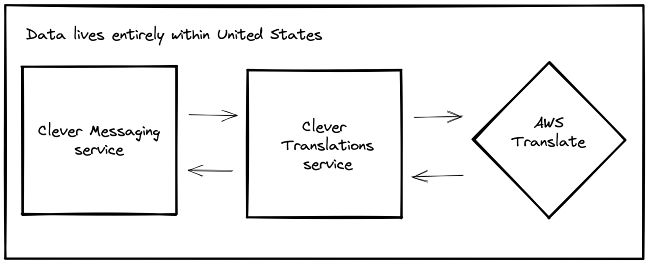
Data lives entirely within United States
Clever Messaging service
Clever Translations service
AWS Translate

Figure 4: Clever's translations are powered by AWS Translate.

As shown in Figure 4, the Clever's messaging services correspond with translation service, which in turn sends requests to AWS Translate [5]. Throughout the entire translation request process, the message data is guaranteed to remain within the United States, because our services house data and operate within the U.S. regions of AWS cloud, and none of the inbound and outbound communication with AWS Translate falls outside of the U.S. Thus, the translation feature of Clever Messaging complies with the data residency restriction imposed by COPPA.

3. Product Limitations and Future Work

Much of the security and privacy design for this product aligned well with our desired user experience. However, there were instances where our security practices created limitations for users. For example, we know there are teachers who regularly interact with students who aren't explicitly in their classes – for extracurricular clubs, sports, mentorship, and more. Our messaging product often could not accommodate these use cases, choosing overall safety over possibly higher risk use cases.

Our privacy and security design also created some limitations for our internal teams. Notably, we chose not to make the content of student and teacher messages available via our existing analytics tools to preserve user privacy. This made it difficult to iterate on the product, since the way to learn what kind of conversations users were having was via user interviews. Ultimately, we solved this problem by building an internal tool that randomly selects and anonymizes a small number of conversations each day. Access to the tool is available to a select group of internal researchers and is maintained by the security team to ensure role-based access control using allowlists.

Moving forward, we are exploring a number of new features to improve the messaging experience from allowing teachers to create arbitrary groups for group messaging and allowing teachers to share application links via messaging, to teacher-to-teacher messaging. As with our previous features, we plan to thoroughly analyze the risk of harm and how to mitigate it as we allow greater functionality.

In conclusion, when designing products for children within online school environments, thorough thought experiments and beta testing should be done in potential risk areas to fully create a secure messaging product that respects privacy. With the multifaceted nature of online education, the threat models should reflect not only the concerns of students and teachers, but also those of many other participants, like guardians and teaching staff, that make online learning possible.

4. References

1. Clever Messaging https://support.clever.com/hc/s/articles/360045714731

2. Levin, Douglas A. "The state of K-12 cybersecurity: 2020 year in review." K-12 Cybersecurity Resource Center (2021).

3. Classdojo Translate Blogpost, https://blog.classdojo.com/introducing-classdojo-translate

4. Children's Online Privacy Protection Rule ("COPPA") https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa

5. AWS Translate, https://aws.amazon.com/translate/faqs/

6. Section IV., User Contribution, Clever Terms of Service.

https://clever.com/trust/terms

7. Clever Secure Sync,

https://clever.com/products/rostering

8.Antivirus for Amazon S3

https://bucketav.com/help/setup-guide

9. 18 U.S.C. § 2258A - Reporting requirements of providers,

https://www.law.cornell.edu/uscode/text/18/2258A

10. To learn more about CSAM, surrounding laws, and ways to help visit: https://www.missingkids.org/home