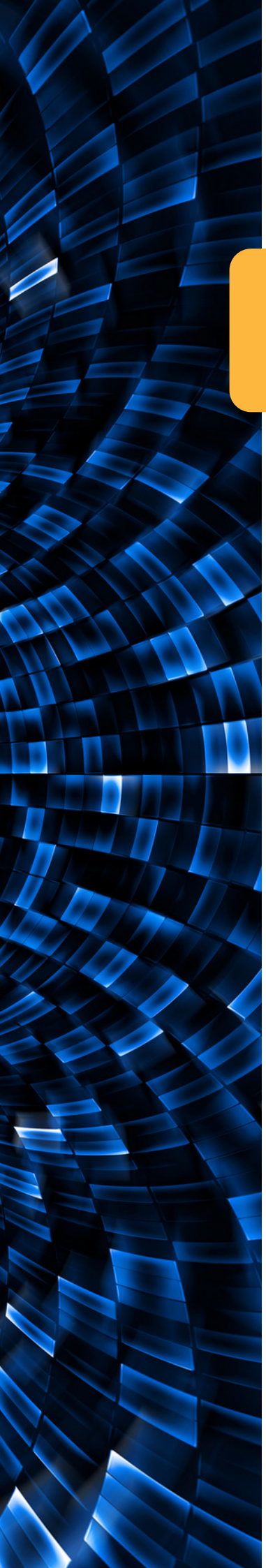

CASE STUDY

POLICY
SIIA

POSITIVE DATA PRIVACY BEST PRACTICES

After April showers, the world sees new data superpowers…

This spring, we are showcasing companies that have launched innovative solutions and best practices for secure and responsible data use. These companies are not just supporting their customers, but providing socially beneficial uses that have a positive impact on the community – from human rights efforts, to improving personalized learning and educational outcomes, to combating deep fakes, to building conscious data practices into the digital ecosystem.

Highlights about each:

- **Meta** demonstrates the benefits of end-to-end encryption in its platforms, which have an intrinsic impact and positive benefit on human rights – including important benefits for individual privacy, freedom of speech, and more.

- **Riiid** focuses on using deep AI solutions to support personalized learning and identify real-time opportunities to increase student engagement in a digital learning ecosystem.

- **Adobe** co-founded and is supporting the development of the C2PA standards, which released version 1.0 of its technical specification for digital provenance this year. The standards will empower content creators and editors worldwide to create tamper-evident media, by enabling them to selectively disclose information about who created or changed digital content and how it was altered.

POSITIVE DATA PRIVACY

BEST PRACTICES

1. META ADVANCED THE BENEFITS OF END-TO-END ENCRYPTION ACROSS ITS PLATFORMS, RESULTING IN EXPANDED INDIVIDUAL FREEDOMS.

About Meta: Meta's mission is to empower people to build community and to bring the world closer together. Meta connects people through building technology and pushing the boundaries of innovation to connect the metaverse. Over 10 million advertisers, mostly small and medium-sized businesses, use Meta's ad tools.

Meta has worked to expand and strengthen the use of end-to-end encryption for its Whatsapp, Messenger and Instagram services. Fortunately, the practice of end-to-end encryption appears to offer critical benefits for protecting human rights and can also address adverse human rights impacts that may arise in environments where end-to-end encryption is absent. A report by Business for Social Responsibility (BSR) recently studied Meta's approach, by analyzing how encryption impacts rights codified in international human rights instruments, including the Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR), the International Covenant on Economic, Social and Cultural Rights (ICESCR), and more. As a result of the analysis, BSR has recommended that Meta continue to leverage end-to-end encryption.

End-to-end encryption is described as "scrambling a message so that it can only be deciphered by the sender and recipient." The company that is providing the service (server) cannot see the message. Therefore, encryption offers enhanced privacy protections that are beneficial and impactful for human rights, such as increasing access to information and allowing greater freedom of expression for individuals. For example, think about a country that regularly arrests residents for speaking out against the government. Through the use of end-to-end encryption deployed on a messaging app, these residents could communicate securely and reach larger segments of the population to get help and protection, which offers critical human rights benefits in this situation.

Traditionally, the debate on encryption appears to pit privacy against security. Through the BSR report, this myth is dispelled. As the report suggests, there are six connected reasons why end-to-end encryption should play a vital role in society's overarching strategy to "protect, respect, and fulfill human rights in today's political, social, and technical context".

POSITIVE DATA PRIVACY

BEST PRACTICES

Meta

continued:

- First, end-to-end encryption should be seen as a clear solution with regard to securing the digital ecosystem, especially in light of growing, technically sophisticated threats.

- Second, this year has demonstrated an uptick in the presence of authoritarian governments, who are severely restricting civil engagement. Encryption is an "organized" solution that can challenge the harsh limitations on political rights and civil liberties.

- Third, advanced social media monitoring programs that are part of these authoritarian regimes are increasingly taking place in digital environments, through "surveillance, spyware, and other methods to turn online spaces into more hostile environments".

- Fourth, it is easy to see that there are more private communications taking place now after COVID-19, than ever before. And some may argue that that trend is not going to reverse.

- Fifth, in a global world, users are connected with a host of other users – those in low-risk environments (i.e. including rule of law/due process/strong privacy protected environments) and higher-risk environments. This means encryption can solve an important information security asymmetry issue, to ensure a safer environment for all users.

- Sixth, privacy and security through encryption should allow for a more equitable and democratized digital ecosystem, where tools that ensure safety are available to everyone – whether an individual is technologically savvy or not. This is particularly important for underrepresented communities who need these additional supports and digital inclusion tools, so that they are not taken advantage of because they are more vulnerable and lack the necessary supports to succeed online.

The report concludes that encryption offers enhanced protection of free expression and is of particular value to companies like Meta, which has over 2.8 billion users and therefore can be the major target for numerous bad actors. The report dives into recommendations for Meta that could also be used by other companies, which include strategies for product, process, product policy and public policy – to proactively detect and mitigate human rights risks and ensure consistency when encryption is implemented.

POSITIVE DATA PRIVACY

BEST PRACTICES

2. RIIID USES FORWARD-LOOKING RESEARCH TO PROVE THE REAL-WORLD VALUE AND COMMERCIAL EFFECTS OF DEEP LEARNING AI PREDICTION MODELS THAT SUPPORT STUDENT LEARNING.

About Riiid: Riiid is a leading pioneer in AI solutions for education, named in the 2021 CB Insights AI 100 list of the most innovative AI startups. It is a global organization of AI researchers, engineers and solution developers fully committed to and passionate about transforming how people learn from AI innovations.

Data from standardized tests and national, reputable surveys like the NAEP demonstrate a general decline in US educational outcomes, especially as it concerns basic academic skills training and preparedness. The outcomes have only been worsened by the pandemic, because US education environments are fraught with teacher shortages and bigger class sizes. Personalized learning and formative learning have been brought up in the national conversation for at least two decades. But, personalized learning and formative learning never really lived up to the promise, which is why the US education environment remains at a standstill. Cue the entrance of the new learning ecosystem: one where real personalized learning is possible, thanks to advances in deep learning AI.

Riiid was founded in 2014 to help students prepare for high stakes tests. Riiid's Santa app was initially used to prepare students for the TOEIC, an English language proficiency test, and grew considerably in popularity. Riiid is now offering the AI algorithms it developed for the Santa App as a service to companies involved in education and personalized learning. In 2020, Riiid conducted a case study, which verified that deep learning AI truly manifests into user value. The study was an A/B test among 78,000 Santa TOEIC users. The experimental group used a deep learning algorithm, while the control group used a classical algorithm. The test proved that deep learning led to more motivation and engagement, which in turn, leads to more personalization to support mastery of online content, which thus resulted in better scores. Data from the case study also demonstrated that accurate score predictions based on deep learning have a positive impact on user confidence in learning tools, increasing their learning motivation. Riiid remains grounded in cutting edge research to improve its current technologies and develop new, beneficial technologies that push the boundaries of educational achievement.

3. ADOBE ADVANCES NEW STANDARDS TO COUNTER DECEPTIVE INFORMATION AND THE DEEP FAKES MOVEMENT

About Adobe: Creativity drives the work at Adobe. Digital experiences are being refined by game-changing innovation. To shape the next generation of storytelling and categories of business, Adobe connects content and data through new technologies.

The deluge of digital content and rapidly advancing technology in today's digital ecosystem has caused consumers to be mistrustful of what they see online. Deceptive content, such as deepfakes, can be indistinguishable from the real thing, so establishing the source and history (or provenance) of media is critical to build transparency, understanding, and trust. The Coalition for Content Provenance and Authenticity (C2PA) -- an organization established to provide publishers, creators, and consumers with flexible ways to understand authenticity and provenance across various media -- released version 1.0 of its open technical specification for digital provenance. Adobe is an important stakeholder shaping the work at C2PA to combat the rise in disinformation worldwide.

The new C2PA open standard is the first of its kind and is empowering content creators and editors worldwide to create tamper-evident media, by enabling selective disclosure of information about the creation of digital content and any alterations that were made. The C2PA's work involves industry-wide collaborations focused on digital media transparency aimed at accelerating progress toward global adoption of content provenance. This C2PA specification will provide platforms with a method to define what information is associated with each type of asset (e.g., images, videos, audio, or documents), how that information is presented and stored, and how evidence of tampering can be identified. As an open standard, it can be adopted by any software, device, or online platform and by regulatory bodies and government agencies to establish standards for digital provenance.