

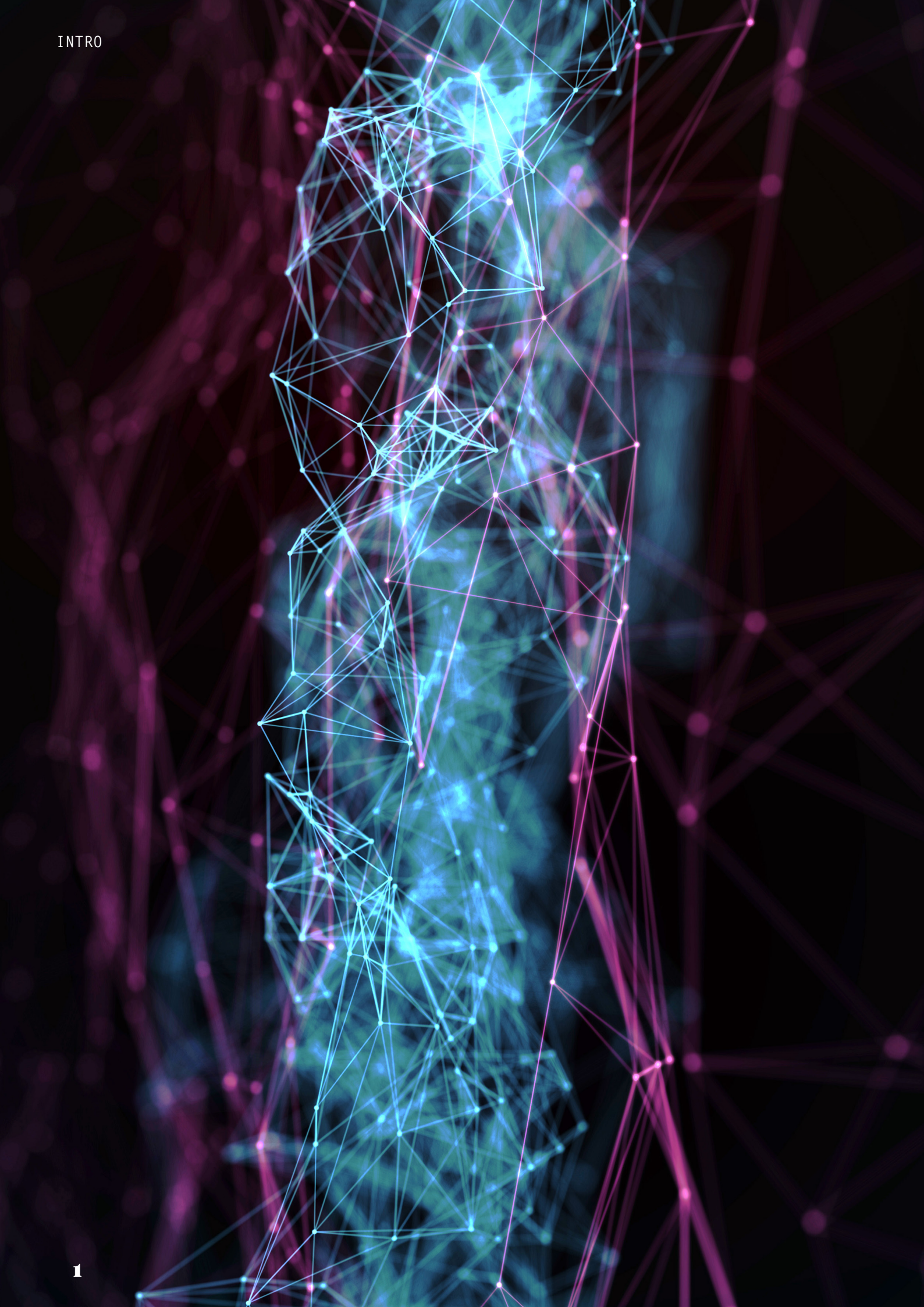
H
I
D

D
E
N

L
A
Y

E
R
S

YOUR QUARTERLY TRANSATLANTIC TECHNOLOGY NEWS
February 2022



In this inaugural edition of Hidden Layers, we discuss some of the main tech policy discussions that occurred at the end of 2021 and early 2022, including the U.S. and EU's approach to regulating Big Tech and Facebook whistleblower hearings, the U.S.-EU Trade and Technology Council, privacy legislation on both sides of the Atlantic, and a debate over the use of artificial intelligence for mass surveillance.

REGULATING BIG TECH & THE FACEBOOK WHISTLEBLOWER

The European Union (EU) has for several years been establishing itself as a leader in technology regulation by going after Big Tech companies and reining in the power they hold in the European market. The EU's most recent move, the Digital Services Act (DSA) and Digital Markets Act (DMA), are a significant step towards updating tech policy in Europe. The DSA would require tech companies to disclose details concerning their algorithms and content moderation practices to regulators, while the DMA would have the authority to set new competition regulation and break up large tech companies that violate antitrust laws.

The DSA and DMA could become law as early as this year. When asked about the DSA and DMA timeline at an [Atlantic Council event](#) on January 12, Cédric O, French Minister for Digital, said Macron's government is hoping they can close the deal before the end of the French EU Council presidency, coinciding with France's presidential elections in April. However, several [member states have opposed this timeline](#) arguing it is not realistic. In comparison to the EU, the U.S. government is lagging behind, often criticized for wagging its finger at tech companies without taking any concrete action. The shift in tone during congressional hearings this past year, however, suggests that the U.S. government plans to increase its pressure on tech companies, both on the antitrust and consumer protection fronts.

Facebook whistleblower, Frances Haugen, a former Facebook employee who leaked internal documents to the Securities and Exchange Commission (SEC) and The Wall Street Journal, contributed to the change in tone towards tech companies on both sides of the Atlantic as the leak led to intensified calls for new legislation aimed at Silicon Valley. In her [congressional testimony](#), Haugen disclosed that Facebook (now called Meta) has repeatedly misled the public and governments about their knowledge of how its various platforms harm children and spread extremist content. Haugen added that the company has the means to make its platforms safer but will not make the necessary changes because ["they put their astronomical profits before people."](#)

Facebook's reaction was to ["spin the politics"](#) and divide lawmakers along party lines, feeding each party different stories to prevent bipartisan regulation against social media companies. These lobbying efforts, however, had the opposite effect. On October 5, two weeks after the Facebook files were leaked, Democrat and Republican members of the Senate Subcommittee on Consumer Protection, Product Safety, and Data Security held a [hearing](#), where members accused Facebook of concealing and ignoring the harmful effects of Instagram, one of the platforms owned by Facebook, on the mental health of children and teens. The hearing immediately started trending on social media as Sen. Richard Blumenthal (D-CT), Subcommittee Chair, asked Facebook's head of safety, Antigone Davis, whether Facebook would commit to ending "finsta," which he described as a service provided by the company. Davis corrected the Senator, explaining that finsta is not a service but slang for a "fake Instagram" account that young people use to share content with a smaller group of friends. Senator Blumenthal's error set off a wave of witty tweets and [raised questions](#) about whether Congress was too old or too clueless to regulate Big Tech. This is not the first time a senator's gaffe has led to a hearing about Facebook going viral. Many will recall Mark Zuckerberg's infamous ["Senator, we run ads"](#) line from the Cambridge Analytica hearing in 2018.

On October 14, following Haugen's testimony before Congress, Democrats on the House Committee on Commerce and Energy introduced the [Justice Against Malicious Algorithms Act](#), new legislation to reform Section 230 of the Communications Decency Act, which currently protects internet platforms from legal liability for the content released by their users. The proposed bill would remove absolute immunity when an online platform "knowingly and recklessly uses an algorithm or other technology to promote content that materially contributes to physical or severe emotional injury." Additionally, Senators Amy Klobuchar (D-MN) and Chuck Grassley (R-IA) [announced plans](#) to introduce a bipartisan bill that would prevent dominant digital platforms owned by Big Tech companies from abusing their market power and favoring their products over third-party vendors. The legislation targets companies like Google

and Apple and goes in the direction of Europe's DMA.

By the end of October, while Facebook announced its plan to hire 10,000 EU employees to build its metaverse, Haugen made her way to Europe. She [testified in front of the British Parliament](#) on October 25 to provide evidence for the UK's Online Safety Bill and encouraged lawmakers to create specific guidelines for risk assessments that lawmakers expect social media platforms to carry out. Two weeks later, Haugen gave a similar [testimony to the European Parliament in Brussels](#) and provided insights into Facebook to help EU lawmakers as they refine the DSA.

Haugen said the DSA has the potential to be a [global gold standard](#) and inspire other countries, including the U.S., to pursue new rules that could safeguard democracy. However, she warned the EU against creating loopholes in the DSA that would allow companies like Facebook to avoid transparency and accountability. Lastly, Haugen mentioned that Facebook was committing worse infractions than its competitors, and in trying to punish Facebook, members of the European Parliament (MEPs) should not punish the entire industry.

The EU Parliament showed some growth since they last questioned Zuckerberg in 2018. According to [Politico](#), the EU's approach and line of questions previously showed a lack of expertise and understanding of technology. However, this time MEPs asked more technical questions concerning automated content systems, encryption, and interoperability. This is also a learning opportunity for the U.S. Congress. By acquiring a deeper understanding of the technology they are regulating, legislators will be in a better position to ask effective questions the next time they have a high-level executive in the hot seat.

To learn more about technology regulation in the U.S. and Europe, read [Cross-Cutting Currents](#), a 2022 Transatlantic Primer covering the biggest challenges facing the U.S., Germany, France, Italy and the UK.



U.S.-EU TRADE AND TECHNOLOGY COUNCIL (TTC)

During the [TTC's inaugural meeting](#) in Pittsburgh on September 29, U.S. and EU leaders identified five issue areas that the various working groups will focus on until their next meeting in spring of 2022. The main tech issue on the agenda is greater transatlantic cooperation on artificial intelligence (AI).

In their [Statement on AI](#), the U.S. and EU recognized that while AI offers great benefits to citizens, transforms industry, and improves quality of life, if misused, AI has the potential to threaten fundamental freedoms. Therefore, the two parties agreed to develop and implement innovative AI systems that could be trustworthy and respectful of universal human rights and shared democratic values. They also decided that policy and regulatory measures should be proportionate to the risks posed by the different AI applications. Both parties agreed to explore cooperation on technologies designed to enhance privacy protections and to undertake an economic study examining the impact of AI on the future of work.

The TTC's Statement on AI also expressed significant concern over authoritarian governments' use of social scoring systems that aim to implement social control at scale. TTC leaders argue that these systems pose threats to fundamental freedoms and the rule of law by silencing speech, punishing peaceful assembly, and reinforcing unlawful surveillance systems.

On technology standards, the U.S. and EU said they support the development of technical standards that are in line with their core values and recognize the importance of international standardization activities underpinned by World Trade Organization (WTO) principles. Additionally, the misuse of technology working group agreed to build an effective mechanism to respond to internet shutdowns in conjunction with the G7 and other like-minded countries, take steps to protect human rights defenders online, and address disinformation and foreign interference with democratic processes. The working group will also address social scoring systems and collaborate on

projects furthering the development of trustworthy AI.

In addition to the TTC, the U.S. and EU held on December 7 the first meeting of the [Joint Technology Competition Policy Dialogue \(TCPD\)](#), which focuses on developing common approaches and strengthening cooperation on competition policy and enforcement in the tech sector. During this dialogue the European Commission, U.S. Federal Trade Commission (FTC), and the U.S. Department of Justice addressed the importance of well-functioning and competitive markets, and common challenges in competition enforcement in digital investigations, such as network effects, the role of big data, and interoperability.

To learn more about the structure of the TTC and its working groups, read [The U.S.-EU Trade and Technology Council \(TTC\) in Detail](#).

ON PRIVACY

The U.S. made relatively good progress on privacy at the end of 2021, with the Senate Commerce Committee convening twice to discuss data protection legislation. At the first hearing in September on [Protecting Consumer Privacy](#), the committee discussed the need for a comprehensive federal privacy law and a proposal passed by House Democrats to allocate \$1 billion to a privacy and data security bureau within the FTC. The second hearing in October focused on [enhancing data security](#), how data breaches impact consumers and business, and the need to ensure the FTC is equipped to fight cybercrime and hold bad actors accountable.

The Committee also held three [Protecting Kids Online](#) hearings that addressed children's privacy regulation, including the Facebook whistleblower and Instagram hearings mentioned beforehand, as well as a hearing that called on executives from Snapchat, TikTok, and YouTube to testify. Although Congress has been moving slowly on this issue, children's privacy is a top priority for lawmakers on both sides of the aisle. When asked about her tech priorities for 2022 at the [Consumer Electronics Show \(CES\) on January 6](#), Senator Marsha Blackburn, the top Republican on the Senate Subcommittee on Consumer Protection, said, "You have to put consumer and children's privacy at the top of the list."

After the Committee's discussions on House Democrats' privacy legislation, House Republicans released a draft privacy bill on November 3 that also proposed a national privacy standard. Representatives Cathy McMorris Rodgers (R-WA) and Gus Bilirakis (R-FL) said in a statement that "privacy does not end at state lines and Americans deserve better than a patchwork of different and conflicting state laws." Like the House Democrats' privacy bill, Republicans' [Control Our Data Act](#) called for the creation of a Bureau of Consumer Privacy and Data Security within the FTC, though Republicans claimed their bill offers more specifics about the Bureau's function versus the Democrats' bill.

Although still in early stages, these congressional hearings and proposed bills bring the U.S. closer to where the EU stands on privacy legislation. While the U.S. is unlikely to have a comprehensive federal privacy framework like the EU's General Data Protection Regulation (GDPR) any time soon, Congress is certainly on the right path. The debate over creating a federal privacy framework will become especially important as more states join California in passing state-level privacy legislation. Virginia and Colorado have already passed their own legislation, while [four other consumer data privacy bills](#) were introduced between January 7-12 in Florida, Washington, Indiana, and the District of Columbia. In response to these bills, the [U.S. Chamber of Commerce](#) sent a letter on January 13 to members of Congress urging for comprehensive privacy legislation to prevent an "unwieldy patchwork of state laws."

On the other side of the Atlantic, a [decision in Ireland](#) sparked a debate over how much leeway companies should have to process personal data and the enforceability of Europe's privacy laws. Because Google, Facebook, Apple, Microsoft, and Twitter all have European headquarters in Dublin, Ireland's Data Protection Commission (DPC) is responsible for holding these companies accountable for privacy violations. On October 13, the DPC published a draft decision agreeing with Facebook's assertion that it does not need to ask users for explicit consent to use personal data for targeted advertising, since users consented to the data collection when they agreed to Facebook's terms and conditions. The DPC did, however, find that Facebook was infringing on the GDPR's transparency requirements. This means that Facebook is able to get away with not asking for consent every time it targets users, but the company does need to make its terms and conditions more transparent, so users understand what they are consenting to.

The DPC said it plans to fine Facebook between 28 and 36 million euros for its lack of transparency over users' data, a fine that [according to TechCrunch](#) would take the company just over two

hours to earn back in revenue. Max Schrems, the Austrian privacy activist famous for filing the Schrems I and II cases that rendered the U.S.-EU Safe Harbor Framework and the Privacy Shield invalid, stated, "With this approach, Facebook can continue to process data unlawfully, add a line to the privacy policy and just pay a small fine, while the DPC can pretend they took some action."

In December, Dutch and German MEPs also [expressed disagreement](#) with the decision and asked Didier Reynders, EU commissioner for

Justice, to open infringement proceedings against Ireland over its slow pace and weakness in enforcing the GDPR. In a letter released in early January, Reynders dismissed the MEP's arguments and defended the DPC's decision, stating that the regulators face complex matters and are right to proceed with caution.



TURNING TO AI

Facial recognition technology, one of the many AI applications in the market, has raised increased concern among policymakers in the U.S. and Europe due to its privacy risks. On October 6, the European Parliament voted in favor of a [total ban on the use of automated facial recognition](#) technology in public spaces, noting that citizens should only be monitored when suspected of a crime. MEPs also asked for a ban on the use of private facial recognition databases and predictive policing based on behavioral data, as well as a ban on social scoring systems like those implemented in China, which try to rate the trustworthiness of citizens based on behavior or personality. On November 24, Germany's new government, led by Chancellor Olaf Scholz, backed the EU's decision and included in its [coalition deal](#) a plan to implement a [ban on biometrical facial recognition](#), as well as automated state scoring systems.

The EU Parliament's proposal to ban facial recognition makes sense in the European context as 2021 [surveys show](#) that a majority of Europeans (55 percent) oppose biometric mass surveillance in public spaces. Young people aged 18-34 oppose the use of these technologies even more strongly at 61 percent. The opposite is true in the U.S., where [54.8 percent](#) of Americans agree that the use of facial recognition technology should not be limited if it increases public safety.

These attitudes might be slowly changing, however, as the U.S. government makes more efforts to assess the dangers posed by AI. On October 8, the White House Office of Science and Technology Policy (OSTP) launched a [Request for Information](#) to better understand public and private sector use of facial recognition and other biometric technologies for identity verification and assessment of an individual's mental and emotional state. A main concern for OSTP leaders is that data sets used to train AI models may not reflect the diversity of Americans and could result in algorithmic bias.

On January 10, Senators Jeff Merkley (D-OR) and Roy Blunt (R-MO) also sent a [letter](#) to the new U.S. Customs and Border Protection (CBP) Commissioner Chris Magnus demanding more transparency regarding the collection of biometric data at airports and other U.S. points of entry. The Senators' letter stated, "While it is now common for American citizens to be told their photo will be taken in order to proceed through the customs process, countless Americans are not adequately informed about their ability to opt out of this step...Every U.S. citizen should have the opportunity to make an informed decision whether to have their passport photo manually verified by a CBP officer instead of having their biometric data collected and stored in a manner with which they are not familiar."