Testimony of

Anjana Rajan
Chief Technology Officer, Polaris

Before the
United States House of Representatives
Committee on Science, Space, and Technology
Subcommittee on Investigations & Oversight and
Subcommittee on Research & Technology

Hearing on *"The Role of Technology in Countering Trafficking in Persons"*

July 28, 2020

Introduction

Chairman Foster, Ranking Member Norman, Chairwoman Stevens, Ranking Member Baird, and members of the Subcommittees, thank you for the opportunity to appear before you today to discuss the important role of technology in the fight to combat human trafficking. My name is Anjana Rajan and I am the Chief Technology Officer of Polaris.

Polaris and Our Technology Strategy

Established in 2002, Polaris's mission is to eradicate human trafficking and restore freedom to survivors. We do this in two main ways. First, we provide immediate response to victims and survivors of human trafficking through our operation of the U.S. National Human Trafficking Hotline. The Trafficking Hotline, which is funded in part by the U.S. Department of Health and Human Services, connects victims and survivors of sex and labor trafficking with services and support to get help and stay safe. Second, we take the knowledge and insight that we have gained in the 13 years we have operated the National Human Trafficking Hotline to make long-term systems change. We tackle the underlying systems that enable sex and labor trafficking, and work with financial institutions to make trafficking less profitable and higher risk. Survivors' perspectives inform all of our work.

Polaris is a technology forward, data-driven organization and technology powers our work. Our technology strategy serves the organization's larger strategy in four key pillars. The first pillar is *survivor engagement*. We do this in two ways: first, we derive signals directly from victims and survivors and those who know them in order to understand their situations and needs; second, we deliver value back to them in a trauma-informed, survivor-centered way. We do this primarily by operating the National Human Trafficking Hotline, and we are now exploring new and innovative ways to increase our reach through technology. The second pillar is *data and analytics*. At Polaris, we analyze the data we receive from the hotline, along with other third-party data and open-source intelligence, to derive meaningful insights and trends about how human trafficking works. The third pillar is *tech policy*. There is a strong role for technology in the fight against human trafficking, but it is important that policymakers understand how these technologies can both help or harm victims and survivors, and ways to effectively leverage them ethically. The final pillar is *security*. At Polaris, we think about the complex threats and risks within the human trafficking ecosystem, and we identify strategic ways to protect victims and survivors, our organization, and our mission.

At its core, human trafficking is the business of exploiting people for profit. It is estimated to be a $150 billion a year criminal industry, with 24.9 million victims worldwide. Effectively fighting human trafficking must focus on the broader systems in place that make people vulnerable to sex and labor trafficking. The application of technology should be part of an overall strategy to drive change at the systems level.

Using Encryption to Help Fight Human Trafficking

Human trafficking is about people with power using every means possible to exploit and control those who are vulnerable for their own profit. Survivors tell us that being able to choose when and how they experience interventions - including when law enforcement intervenes - and restoring their sense of

control is paramount to their healing. Technology should not only enable law enforcement to identify traffickers; it should also be used to *put power back in the hands of victims and survivors.*

To pass meaningful and effective legislation to combat human trafficking by leveraging technology, it is imperative for legislators to fully understand how these technologies work and impact victims and survivors directly. One of the technologies that has recently been discussed in this space is encryption, otherwise known as the encoding of information.

Because my background and expertise are in the application of cryptography to human rights and national security issues, I would like to focus my testimony today on the importance of encryption in fighting human trafficking.

In the public debate around encryption, we often only see two sides represented: one side that says we should protect victims and survivors at all costs, even if that means we break encryption to do it, and the other side that says we should protect encryption at all costs, even if that means victims and survivors get hurt.

This is a false dichotomy. There is a third way that can optimize for both virtues because *encryption protects victims and survivors*. And, while we protect the integrity of encryption, we can still hold perpetrators (and the platforms that enable them) accountable for their abuse and exploitation. But doing so will require innovative thinking and an accurate understanding of how these technologies work.

To honor the exploratory nature of this committee hearing, I am proposing three possible ways encryption could be used to help fight human trafficking and support victims and survivors. These ideas are meant to spur a larger dialogue, and would of course require a great deal more consultation with survivors:

- Using **secure multiparty computation** to build safe, survivor-centric reporting channels
- Using **homomorphic encryption** to enable financial institutions to share data in privacy-preserving ways
- Using **cryptocurrency transactions** to map and dismantle human trafficking networks

Using secure multiparty computation to build safe, survivor-centric reporting channels

In order to understand the complexity of the human trafficking problem, we must understand the threats victims and survivors face. The security threat model for victims of human trafficking is very dangerous, uniquely complex, and highly dynamic, and victims face a variety of risks from many types of adversaries. They face prolonged control and manipulation from traffickers and organized crime networks. They face physical, psychological, and sexual violence. They face intimidation from conspiracy theorists who weaponize disinformation in order to thwart their pathways to safety. They may even face threats from law enforcement agencies who arrest them instead of helping them find freedom.

We see this every day at Polaris as we operate the National Human Trafficking Hotline. Victims and survivors often reach out to the Trafficking Hotline unsure about their options for getting help and staying safe. Trafficking Hotline Advocates discuss choices like finding a safe place to stay, obtaining legal assistance, and connecting with a case manager, as well as the option to report to law enforcement.

Especially for those with a history of criminal charges or past negative interactions with law enforcement, reporting can be a daunting experience. It is common for survivors to choose to connect with a service provider for wrap-around support before deciding if they are comfortable reporting to law enforcement. Since Polaris began operating the National Human Trafficking Hotline in 2007, 9,943 situations of likely human trafficking have been shared with the hotline directly by adult victims and survivors. *In only 23 percent of those situations did the victim or survivor consent to or request that the National Hotline provide details about their trafficking situation to law enforcement.*

The problem of low victim and survivor reporting rates can be understood as a game theory problem. Simply put, this means that there is a low incentive for someone experiencing human trafficking to disclose vulnerable information to law enforcement for fear of retribution, but if the person can decide to disclose when they are ready after learning more information about their options, they are more likely to take action. In addition to hotlines, there are innovative ways to use cryptography to empower survivors to take action and seek justice.

A *cryptographic reporting escrow* is an example of a solution for situations in which somebody should report something in order to protect society but may be reluctant to come forward on their own. Such an escrow would be a trusted third-party system (that the government does not own or have direct access to) that allows victims to report abuse and exploitation. The report is only unlocked and given to law enforcement if and when a threshold of severity is met. Cryptographic escrows build trust in a fundamentally new way. Four key principles define such systems:

- *Threshold-based:* one victim's record stays locked until a threshold of risk is met by one or more people;
- *Zero-Trust Network:* the data stored in the escrow is protected from both outside and inside threats;
- *Human Legal Firewall:* the record is unlocked by a person who can establish privilege and block disinformation; and
- *Multiple Calibrated Options:* victims have several holistic options for how they choose to take action.

The underlying technology pinning these escrows is called *secure multiparty computation*. It is a cryptographic protocol that distributes a computation across multiple parties where no individual party can see anyone else's data. I have built information escrows using secure multiparty computation in other use cases, such as combatting sexual assault and countering domestic terrorism, and I believe this technology could potentially be applied to combat human trafficking as well.

Using homomorphic encryption to share financial institutions' data in privacy-preserving ways

Human trafficking is a diverse crime, often perpetrated through complex psychological manipulations, the exploitation of economic desperation, or taking advantage of emotional need. But behind all the complexity, human trafficking is, inherently, a commercial enterprise.

Financial system intervention in human trafficking has the potential to increase the risk for traffickers, reduce the profitability of trafficking, and reduce vulnerability to trafficking within particular

communities. That is why Polaris has partnered with PayPal to create the first financial intelligence unit housed within an anti-trafficking organization. The financial services industry has data that can serve as a unique leverage point which, when properly analyzed, supports both fights against sex and labor trafficking. The use of financial evidence in the criminal justice process could mitigate the burden placed on victims to participate in investigations and prosecutions and facilitate the financial restitution process. Ultimately, Polaris is working toward a world where trafficking in sex and labor will be a less profitable and higher risk business venture.

While data analysis is key to understanding and solving the human trafficking crisis, this vast data is often highly sensitive and has many privacy implications. With financial regulation now mandating the responsibility of financial institutions to proactively spot the warning signs of trafficking, there is increasing urgency to solve this problem.

Homomorphic encryption could be an answer to this problem because it could allow human trafficking researchers to run analytical functions directly on a financial institution's encrypted data without ever seeing the plaintext sensitive data. Homomorphic encryption secures data while it is used, whereas other forms of encryption only secure data while it is in transit or at rest. More importantly, homomorphic encryption can support encrypted analytics, meaning machine learning and artificial intelligence models can be applied to this encrypted data set as well. Since homomorphic encryption is a type of lattice-based cryptography, it provides the additional benefit of being resistant to quantum computing attacks. Therefore, we can continue to accelerate our ability to analyze important financial data to identify and dismantle trafficking rings, while also acknowledging the data's sensitivity and prioritizing privacy during this analysis.

Using cryptocurrency transactions to map and dismantle human trafficking networks

Human traffickers have eagerly adopted the use of cryptocurrencies to finance their operations. Cryptocurrencies, such as Bitcoin, are appealing for two main reasons. First, their decentralized nature means that there is no centralized authority that can shut down accounts or freeze funds. Second, cryptocurrencies provide a certain level of anonymity; one can create a Bitcoin address and receive tokens without needing to provide a valid name or address. According to Chainalysis, a technology company that analyzes blockchain data, there were nearly $1 million worth of Bitcoin and Ethereum payments in 2019 for child sexual abuse material.

The problem of cryptocurrencies has been discussed in many contexts, including domestic terrorism and violent extremism. On January 15, 2020, the House of Representatives Committee on Financial Services held a hearing entitled, "A Persistent and Evolving Threat: An Examination of the Financing of Domestic Terrorism and Extremism." One of the recommendations presented at this hearing was that cryptocurrency providers should ban extremist organizations, with the intention that cutting off their financial supply would hinder their ability to mobilize effectively. One could argue that a similar recommendation should be made for networks that facilitate human trafficking.

However, there are several limitations to this recommendation. First, cryptocurrency advocates will argue that this violates the intended value proposition of a decentralized currency, and private sector

stakeholders thus are likely to push back heavily on this regulation. Second, such a solution simply treats the symptom, not the root cause; bad actors will continue to find new and illicit ways to finance their operations, and removing access to cryptocurrencies would only impose temporary friction. *Most importantly, eliminating access misses a significant opportunity to leverage this technology's properties to ultimately solve the primary problem of dismantling human trafficking networks altogether.*

The unique properties of blockchain technologies offer a big opportunity to help the fight against human trafficking. While aspects of cryptocurrencies are anonymous, part of what drives consensus around the currency's legitimacy is that the transactions are permanently stored on a public, decentralized ledger. If law enforcement uncovers the Bitcoin wallet address of a person or organization, they can easily trace their entire transaction history with other Bitcoin addresses. With known wallet addresses and their corresponding public transactions, law enforcement agencies can build a dataset of human trafficking buyers and sellers, and ultimately map out the entire network of a human trafficking ring. Additionally, metadata trends can also help law enforcement agencies detect suspicious activity, such as time and size of transactions. This data analysis could be used by law enforcement to build out better risk profiles and have higher success rates in dismantling networks.

Conclusion

Human trafficking is a complex, multifaceted problem that requires nuanced solutions. It is a result of social, policy, and market failures. Technology, at its best, can help rebalance power. However, it is not and should not be treated as a panacea. The unchecked use of advanced technologies - whether it be artificial intelligence, machine learning, facial recognition technology, or others - *have the potential to suppress freedom, rather than restore freedom to survivors.*

We need to design and deploy technology with intention, a clear understanding of the problems they are meant to solve, and the best interests of victims and survivors at the center, ultimately recognizing that their needs and wants are complex and not homogenous.

Thank you for the opportunity to testify on Polaris's approach to using technology in the fight to end human trafficking. I am happy to answer any questions you may have.

Anjana Rajan

Anjana Rajan is a technology executive and entrepreneur whose expertise is applying cryptography to national security and human rights issues. She is the Chief Technology Officer of Polaris, an NGO that uses data-driven strategies to disrupt and prevent human trafficking and modern slavery.

Anjana is the former Chief Technology Officer of Callisto, a nonprofit that builds cryptographically-advanced technology to combat sexual assault. In this role, Anjana led the engineering, security, and design teams, with a focus on building products that protect the privacy of sexual assault survivors. Callisto is funded by Greylock Partners, Y Combinator, and the Skoll Foundation.

Recently, Anjana was a Tech Policy Fellow at the Aspen Institute. During her fellowship, she created policy solutions to create privacy-preserving methods to eradicate mass gun violence caused by white supremacist terrorists. She is also an independent research consultant for the Homeland Security Advisory Council that supports the country's top national security leaders on cybersecurity policy.

Previously, Anjana lived in London and worked at Palantir Technologies, where she built and deployed big data software platforms. At Palantir, she served as a Commanding Officer for a deployment in the Middle East and worked across commercial and international government projects. Prior to joining Palantir, Anjana worked as a technologist at Johnson & Johnson focusing on building new software products across global healthcare markets.

Anjana was a Knight Scholar at Cornell University and received her bachelor's and master's degrees in Operations Research and Information Engineering. Anjana is also a former elite triathlete who raced for Team USA.