**To: Interested Parties
From: Ken Gude
Date: November 29, 2022
Re: How trusted technology can help better protect us against modern digital threats**

Trusted Future recently co-hosted a discussion with the Munich Security Conference (MSC) on cyber and digital threats to the transatlantic community. The event followed a high-level roundtable discussion that MSC hosted in Washington about how the transatlantic community can leverage technology for strategic advantage in the face of current and future technology- enabled threats. While the war in Ukraine was the backdrop to the conversations, the discussions also elevated the critical role of having robust cybersecurity defenses, and, importantly, Ukraine’s innovative, inspiring, and informative use of technology throughout the conflict.

These talks build off a conversation Trusted Future held earlier this year on the sidelines of MSC’s annual conference in Munich in February. While the conversations were held less than a year apart, so much had changed in such a short time. The first event was held on the eve of the Russian invasion. In the time since, the world has watched as Ukraine defied all expectations, with the role of information and communications technology playing an important part.

Rather than seeing oft predicted debilitating cyber-attacks against Ukraine’s critical infrastructure, we saw the ability of intensive public-private defensive planning and operations thwart the attempts by Russian forces to take utilities and other assets off-line. We also saw how everyday Ukrainians harnessed some of the same personal and commercial technologies that they used in their daily lives before the invasion in new and effective ways to participate in their nation’s defense while not becoming actual combatants.

These advanced cyber defense actions were not trivial, and they mattered. Even before the Russian invasion, U.S.-based and other technology companies worked closely with the Ukrainian government to improve and secure the country’s digital infrastructure. Investments in cybersecurity, resilience in infrastructure, use of the cloud, and the redundancy of operations proved critical for Ukraine, allowing the country’s energy networks, banks, and government services to run despite reported attempts at disruption.

**Widespread availability of secure and trustworthy commercial technologies is empowering Ukrainian citizens in new and novel ways.**

One element that stands out is the widespread use of personal technologies like smartphones in the hands of Ukrainian citizens being used and leveraged in meaningful ways. Ukrainian citizens used apps on their phones to organize relief efforts, combat disinformation, protect evacuees, and even report on Russian troop movements. They have used their phones as a window for watching President Zelensky rally his nation and galvanize the world each night with regular video messages. President Zelensky isn’t alone in the use of video. Ukrainian citizens turned to popular smartphone apps to share firsthand videos of what was actually transpiring on the ground, and to document and share evidence of potential Russian war crimes. They not only increased transparency and made it harder to ‘hide’ what’s really going on, but these accounts also helped win the hearts and minds of much of the world.

Everyday citizens also turned to information and communications technologies to coordinate their efforts privately and securely. Early on, many Ukrainians downloaded secure messaging apps, like Signal, to communicate and coordinate information and resistance. Ukrainian volunteers even developed a smartphone app with the ability to report on the location of Russian attacks, tanks, missiles, and drones -- supplementing government intelligence collection. In fact, one MSC leader vividly described what he believed to be the critical technology difference between this conflict versus conflicts of the past. He said it was the Ukrainian grandmother who was now empowered with tools to enable her to look out her window to watch for and report on Russian troop and tank movements with the very same technology she previously carried every day in her purse. The fact that the technology was already widespread, and that there was no need to train people in how to use it, made it even more powerful.

Because of this technological shift, key paradigms are changing. It's no longer just states or even commercial technology providers, but the end users of technology who can help impact the course of the conflict. It elevates the importance of the commercial technologies to both our economic and national security, and it suggests we need to similarly elevate policies to ensure that the West continues to lead the world with robust off-the-shelf technologies that are agile, innovative, secure, trustworthy, and able to provide secure communication wherever it’s needed. In today’s technology-centric world where citizens carry powerful processing and communications tools in their pockets, innovation and ingenuity have moved to the forefront of how we secure our future. This trend will accelerate as we move deeper into applicable emerging technologies, including faster and highly configurable 5G data streams and AI assisted applications and data processing.

**Ukraine’s nimble use of technology has lessons for the world and ensuring trust in our technology is a key enabler.**

It was clear from the MSC talks that the transatlantic community can now better position itself to leverage our commercial technological advantages to overcome our shared challenges, and better position ourselves for success. Some suggested the transatlantic community needs to focus on concrete ways to better leverage our top technology developers so we can continue to out-innovate, out compete, and out-smart our potential adversaries. It is a key area for transatlantic cooperation. The very fact that widely available consumer products – largely developed in American and European innovation hubs – are playing a significant role in Ukraine, demonstrates that the ingenuity and creative technological solutions we develop today can be even more critical to our success tomorrow.

One government official who participated in the discussions highlighted the importance of secure personal technologies, saying that for the person’s highly sensitive government work, their agency secured their data and communications. But for their – still quite meaningful – personal data and communications, they rely on trustworthy personal technologies to keep them and their family secure and communications private. Often, these personal- or commercial- technologies play roles in both official and personal networks and communications. The tech industry ‘builds-once-and sells-globally,’ and the same phones, routers, firewalls, or applications that are used by consumers are used in companies, critical infrastructure, military, and intelligence networks. Driving security and trust into all is therefore critical, as is making sure that policy makers do not unintentionally do anything to make these technologies less secure or trustworthy – it’s a global connected ecosystem.

It means that, today, we need our commercial off-the-shelf technologies to be infused with strong security and robust privacy features and ensure that innovators are able to continuously advance increasingly capable technologies. Whether it’s a Ukrainian protecting their sovereignty in the streets or an average American consumer – we all must be able to benefit from a robust and trustworthy technology ecosystem. We all must be able to trust that our devices, apps, platforms, and services are safe, that our data is secure, and our privacy is always protected.

**Going forward, governments need to further leverage private sector technology leadership to ensure we have the economic, security, and technology advantage today and tomorrow.**

To build truly secure and resilient systems, we can’t just rely on government solutions alone. Governments and policymakers alike need to leverage and accelerate our technological advantages and leadership. It requires making sure we continue to lead the world in the technologies of tomorrow by investing in innovation, strengthening our technology supply chains, boosting our semiconductor manufacturing abilities, building out innovation hubs, and fostering the high-tech workforce needed for tomorrow.

**The foundation of trust needs to be baked into both our technologies and our technology making process.**

We also need trust baked into both our technologies and the foundations of our policymaking process. One point that came up repeatedly throughout the conversation is the need to evaluate the security, privacy, and other impact of new policy proposals. It means we need policymakers everywhere, including those in the U.S and EU, to advance technology policy proposals that elevate privacy and security standards. At the same time, policymakers must avoid actions that could unintentionally undermine the foundational protections consumers need for their privacy and security today, and that may help ward of threats from authoritarian regimes tomorrow.

One way to bake trust into the policymaking process is to institute a comprehensive technology assessment of the privacy, security, and safety impacts of proposals prior to enactment. Congress today, for example, performs a budgetary impact assessment (a ‘score’) before passing legislation. Local leaders similarly perform an environmental impact assessment before building a new project. A similar assessment on trust and security for technology policies can help improve outcomes and reduce the chances that policymakers will inadvertently impede our ability to harness future technologies. Such an assessment would also ensure that new policies do not actively make devices and systems less trustworthy, less secure, less reliable, or less resilient.

Empowering consumers with powerful and capable technologies requires ingenuity and innovation from all sectors of society. And there is no time like the present to get started.