Call for Position Statements - *Privacy & Pandemics: Responsible Uses of Technology and Health Data During Times of Crisis* — An International Tech and Data Conference

Position Statement – Rina Shainski, Co-Founder and Chairwoman, Duality Technologies

Data has been called 'the new oil' for its vast contribution to economic growth, and is also the lifeblood of advanced research and development. But when the COVID-19 pandemic swept across the planet, all too frequently, the vital data necessary for managing the crisis more effectively and advancing research has been inaccessible due to data privacy regulations -- especially around sensitive personal information. The smart utilization of crucial and "hyper-sensitive" health and location data related to the coronavirus could help us control, manage and understand countless aspects of the disease -- including where new hotspots are likely to emerge, how it is transmitted, how it affects the human body, and which methods of treatment are effective for different patients. But data privacy concerns have hampered our ability to fully harness big data in order to help manage the ongoing health crisis and create a safe pre-vaccine routine that would allow us to re-ignite the economy.

The collection and analysis of personal healthcare data, and ability to share it across institutions and even borders to quickly glean vital insights has been impaired by growing privacy regulation protecting our personal data.

The friction between data utility and data privacy is not new, and has been developing side by side with the growing amounts of data we are producing at any given moment. With the emerging pandemic, this tension has morphed into a critical dilemma ostensibly pitting public health against individual privacy.

On the one hand, more and more forces in the ever-expanding data economy seek to harness the benefits of big data sets, not only to monetize this increasingly valuable commodity but also to promote vital research and technological breakthroughs across a range of fields. On the other hand, governments and regulators -- alarmed by the ease with which sensitive personal data can be transferred to and potentially misused by third parties -- have restricted the flow of data through increasingly stringent privacy laws such as the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA).

The Covid-19 crisis has only served to highlight the problematic nature of this tension and make clear that collaboration is essential to every application of data science, including disease containment and research. Given the scale of the current crisis, we need to address this challenge now so that data can become a key driver of our response to the pandemic.

Technology is at the root of the ongoing data explosion and the growing data privacy quagmire, and technology can also help untie this knot. But how?

Privacy-Enhancing Technologies (PETs) have the ability to reconcile these conflicting needs and allow society to reap the benefits of sensitive personal data -- without compromising our personal data privacy. Privacy-Enhancing Technologies based on

Homomorphic Encryption (HE) can bring about a new paradigm, enabling secure data sharing while alleviating privacy concerns.

While many of these technologies are ready for market adoption, there have, unfortunately, been many missed opportunities to implement them over the past six months. The pandemic is a wake-up call for public stakeholders and data owners to explore PETs and start deploying them on a growing scale, to better manage the current crisis and enhance readiness for future challenges that will require global cooperation.

Two critical fields in which PETs such as HE could address major challenges in the current and future health crises include:

1. Privacy-preserving contact tracing

During the first months of the pandemic, there have been vociferous debates concerning contact tracing technology, which was often criticized as privacy-intrusive. The decentralized opt-in apps that many countries developed based on the Google and Apple framework are generally considered the “safest” option regarding privacy. However, they often leave authorities without the necessary data to develop and implement effective strategies to contain the virus.

Homomorphic Encryption allows multiple parties to pool and analyze personal data *while it remains encrypted* and thus private. In this way, HE maximizes sensitive data’s potential, preserves individual privacy, and, crucially, remains compliant with privacy legislation. Prominent legal opinions suggest that homomorphically encrypted data can no longer be considered ‘personally identifiable information’ (PII) and is therefore exempt from privacy regulations, yet compliant with them. In other words, we can protect our data - and use it too.

When leveraged for privacy-preserving contact tracing, HE can enable governments to utilize data held by telecom and healthcare providers and access more complete datasets than those held by decentralized opt-in apps -- without violating individual privacy.

2. Medical research

PETs could also significantly enhance researchers’ ability to respond to the pandemic. As scientists continue to investigate the nature of the novel coronavirus, their research must draw on datasets derived from real-life patient information. However, legitimate privacy concerns and regulations have prevented individual health data from being aggregated and analyzed in settings that involve multiple parties -- as is required for advanced medical research.

HE has already demonstrated its utility in cutting-edge research into the relationship between genomics and Covid-19 susceptibility. In May 2020, a team of data scientists and researchers published an article in PNAS detailing how privacy-enhanced genome-wide association studies (GWAS) carried out on over 25,000 individuals using HE can yield results significantly faster than previously used privacy-preserving computation methods, making it far more feasible for practical healthcare research covering large data sets. GWAS can yield insights into a range of diseases. Since privacy protection is critical to research based on genomic data --

arguably the most sensitive data type of all -- this technological advance can be a gamechanger.

In addition, privacy-preserving Machine Learning capacity based on HE is currently being developed to train models on sensitive genomic and clinical data pooled from various sources without ever exposing the data -- taking privacy enhanced analytics capabilities even one step further.

Technological methods to harness data and make significant breakthroughs in the fight against Covid-19 are ready to be utilized. The onus is on policymakers and regulators to endorse their use more systematically and enhance our ability to respond to the huge challenges posed by the pandemic. Privacy regulation is advancing, but the differences in legislation across jurisdictions is becoming further entrenched, leading to friction between competing privacy frameworks that can severely impede data-driven research across geographies. The UK's new data strategy has taken the lead, calling for PETs to be deployed to 'facilitate data sharing in ways that can improve privacy and in so doing build trust.'

PETs have the capacity to create a new paradigm by which data privacy and data utility need not be irreconcilable. With the ongoing threat to public health and subsequent financial fallout, now is the time for policymakers and regulators to endorse, actively promote and fund the use of Privacy Enhancing Technologies so that industries and authorities are able to leverage data in the fight against the pandemic.