DATA PRIVACY INSIGHTS · 3 MIN READ

Data Privacy and Technology: Key Issues Missing from the Center Stage of Politics

KON LEONG · APRIL 28, 2020

Albert Einstein was said to have remarked: “It has become appallingly obvious that our technology has exceeded our humanity.” This was well before the age of IT. His observation would have been prescient, though.

Witness the searing pace of change in information technology and juxtapose that against the slow-motion crawl of our political and legislative systems in understanding and adapting to it. Over the past few years, information technology, analytics and related spaces have advanced by leaps and bounds, mostly behind the scenes, only emerging into the national spotlight for events like major data breaches, social media scandals, and electoral interference.

This is just the tip of the iceberg. Petabytes of personal information are created, collected, and analyzed every day by corporations, governments and, of late, election campaign managers. Curiously, even as the Democratic presidential primary wraps up and the general election gets closer, political attention and press coverage on data privacy remain mostly absent. On the federal level, privacy is very much a mixed picture, with courts indicating confusing stances on privacy issues, while the same applies to the political arena where political candidates outline positions on privacy which span the spectrum from passive to aggressive. At the state level, many, including California, have followed suit behind the EU’s General Data Protection Regulation (GDPR), which grants users the right to determine how their data is accessed, used and retained. At every level, however, policy makers and enforcers alike often miss the fundamental but nuanced issues facing privacy.

For example, to implement privacy, there are two basic approaches: know nothing or know everything. Knowing nothing is simply not feasible today, where compliance and litigation requirements compel organizations to know the content of their data. That then forces us to know everything about our data, in order to identify which data is private, so as to enforce usage restrictions. Which then leads us into a bit of a quandary where, in order to provide you privacy, there must first be intrusive knowledge of your data.

The CIA's classified information system exemplifies this privacy paradox, in which users can see only what they are authorized to see, while, at the same time, it could be viewed as perhaps the most intrusive information gathering and classification apparatus.

This quickly leads to other paradoxes. In fact, one could say that privacy regulations enable the police state. If you think this is farfetched, think of private information as nuggets of gold. Today, they are buried in the dirt and not readily accessible without a whole lot of effort to mine and sift. However, recent privacy laws now require a system that conveniently classifies private data, effectively drawing a convenient map of where all the "nuggets" are. The implications are far-reaching. Given the power, how many governments could resist reaching for this data? Sadly, human history shows little success in sustained oversight and how absolute power corrupts absolutely. Recent political events across countries and continents are replete with examples of abuse of power with overnight suspension of human rights by fiat including unilateral declarations of "emergency law."

Exacerbating this risk is faster-paced technology development in increasingly invasive areas, such as biometrics. It's one thing to lose a credit card to theft; one can always replace it. However, it's not so easy to change one's fingerprints or iris. And we have only just begun long-distance invasion of privacy now made possible through developments such as facial recognition and DNA databases.

To underscore the cumulative impact on a free society, I posed a hypothetical question to a recent panel on Big Data: If we could send today's technologies on surveillance and data analytics back in time to WWII, would there have been a significant resistance movement? The silence following the question was deafening.

With so much at stake, how then do we fully harness information while still providing privacy protection and ensuring sustained supervision with appropriate checks and balances? A key concept of good information governance is prescribing a "Plan B" when the data falls into the wrong hands. Thus far, such remedial Plan B's

are seldom mentioned. Apart from fines, there is rarely anything to be done to undo the data leak, or "un-ring" the bell.

As technology growth accelerates, it's hard to say precisely what advancements will arise five or ten years from now. Without a substantial shift in attitude, however, our privacy protections will continue to erode and the legislative process will lag dangerously behind new developments in technology. Until the potential for abuse of power hits home, politicians will continue to only address data privacy superficially, with the sole exception of cases where it directly impacts their electoral prospects.

> Data #privacy is still not focus issue in presidential #election2020 despite 75% of Americans asking for more government regulation of consumer data. #respectdata
>
> Click to Tweet

Thus far, data privacy is not yet center stage in the 2020 presidential race, despite the fact that 75% of Americans say there should be more government regulation of consumer data, according to a study published by the Pew Research Center. If our politicians fail to adequately address this issue, the window of opportunity to fix it may close, and with it, the proliferation of our private information may become truly irreversible.

TAGS #DATA PRIVACY