- PDF
- Send to a friend

On Technology, Security, Personhood and Privacy: An Appeal

Essay by John Clippinger, June 10, 2008

American democracy has weathered many storms in its 239 years. Its survival and prosperity are consequences of both good fortune as well as the remarkable foresight and common sense of its Founders.

However, a new kind of challenge looms on the horizon, unanticipated by even the most prophetic of the Founding Fathers. It is Technology, more specifically, digital technology, which both offers the promise of unfettered communication, learning, and global commerce, and the prospect of a Panopticon-like State. Two extremes, two doors; each with radically different outcomes. Yet it is the latter choice that is currently championed by the American administration, as well as by its English, European, and Asian counterparts. Buttressed by video clips of angry, bearded terrorists, and a steady refrain of color-coded warnings, a State of omniscient surveillance has emerged as not just a patriotic necessity, but as an inevitability.

But at what cost to our liberties? Must society choose between individual freedoms and public security? Today the threat is not of a marauding army spilling over our ramparts in the dead of night, but a failure to recognize the “bad guy”— not just at our “walls”, but within our walls. .

Yet invasions of individual privacy are inherently an affront to the sacred, social contract of any Democracy, and therefore, not to be undertaken lightly. The presumptive and defining impetus of any authoritarian regime is to know everything about its subjects, to conduct a continuous campaign of “total awareness” where it is assumed that the State can be trusted and its subjects cannot. In a Democracy, arming a sovereign– even an elected one – with undue powers is to risk turning the State against its people, thereby undermining a fundamental premise of Democracy: We the People.

But, how do we proceed when national security does require the identification of potentially threatening individuals? Shouldn’t those with nothing to hide be willing to trust the government? Shouldn’t every citizen be willing to cooperate with measures that protect the security and liberty of all people? Is not a diminished sense of privacy and autonomy a small price to pay for national security?

To set up a choice between greater freedom and greater security is to create a Hobson’s Choice. If one has to relinquish one’s personal freedoms in order to be secure, then the very rationale for those freedoms is abrogated. Moreover, without trust between the individual and the state, there can be no basis for a social contract. Rather, if there is to be a true and durable social contract, then each party has a living obligation to the other to ensure the inalienability of liberty and security.

How might this be achieved? The remedies lie in principles, practices, and indeed, technologies never imagined by the Founding Fathers. The same technology that gives us the ability to communicate and congregate also gives us the powers to monitor those very communications and to distinguish friend from foe. Imagine for a moment that the eyes and ears of every man, woman and child within a village could be commandeered to watch and report on your every move. Imagine also that they would do so with good intent, but as with all people, their judgments would be fallible. Yet in this instance, their judgments would be deemed definitive.

Imagine then what you would be willing to risk in thought, word or deed. No longer would you be a free citizen. You would be a hostage of the State.

Fortunately, people do not have such powers. But technologies do, and they can be used to watch and listen to and remember virtually everything all the time. Such is the dark side, but it is precisely this seemingly sinister dimension of the technology that, paradoxically, renders it a powerful guardian of democratic principles. While people are inherently incapable of controlling everthing that they see, hear and remember, machines are very good at this, and can embody and enforce policies that can govern precisely what people, companies, and governments can and cannot know about one another.

What this means is that technologies can and should be used to reveal to governments and other authorities only what the governments or authorities explicitly need to know, when they need to know it— without compromising a person's privacy or freedoms. It also means, almost paradoxically, that governments can collect information – non identifying information – about people to track suspicious behaviors to identify malevolent actors. Governments do not have to sacrifice privacy nor individual freedoms to protect their borders and citizenry. There need not be a Hobson's Choice.

In order to bring Democratic principles into the 21st century, they need to be reconciled with - and augmented by— Technology; in this case, digital technology. In other cases, it could be biological technologies. In this particular instance, the ability to project democratic freedoms into a digital future would require that every citizen has control over their personal information. As an expression of this inherent right, citizens would need only disclose the minimal amount of information that a governing or authorizing body requires to perform its duties.

Complementing this inherent right is the obligation of the citizen, whether at birth or through naturalization, to be identified and verified by a government authority. However, this identifying information would not be public in any sense, and would only be obtainable through a search warrant.

Citizens would have multiple, pseudo-anonymous personhoods for various commercial, governmental, and non commercial purposes, and these could be monitored through consent and statute, thereby enabling and encouraging the free and protected flow of information.

In some quarters, such an interjection of digital technology into matters of commerce, civil liberties and governance has been met with suspicion, as if it were some kind of unnatural additive, masking potential carcinogens. While that prospect is ever present, digital technology will be an integral component of future democracies, and if we, as members of a global community, show the same perspicacity, commitment, and wisdom as the Founding Fathers, it may be possible to accelerate the birth of authentic democratic institutions, not just within the United States, but throughout the world.

John Clippinger is a senior fellow at the Berkman Center where he works on the development of Higgins – software that gives people control over their personal information. He co-founded the Social Physics project *to research the impact of trust, reciprocity, reputation and social signaling on the formation of digital institutions. He is the author of* A Crowd of One: The Future of Individual Identity *(2007).*

All Security Essays

Anonymity

- Anonymity on the Web
  by The Cheshire Cat

Privacy

- The Right to Privacy. Again.
  by Dembitz
- On Technology, Security, Personhood and Privacy: An Appeal
  by John Clippinger

Protection from Harm

- What Would a More Secure Future Look Like?
  by David Clark
- Malware: The Great Equalizer
  by Beau Brendler

View all thematic areas »

Source URL:
http://publius.cc/technology_security_personhood_and_privacy_appeal#comment-0