KEYNOTE ADDRESS

THE DIGITAL FOREVERMORE

Thomas J. Ridge *

We now live in what I call the "digital forevermore." It was not that long ago that the original computer base data transmission protocol was created simply to facilitate telecommunications between the United States Department of Defense and research universities. While certainly primitive compared to the digital global ecosystem that drives commerce and culture throughout the world today, its core features remain the same. The Internet is an open system based on anonymity. It was never designed to be a secure communication platform.

The opportunities and vulnerabilities within this global network, with electrons racing everywhere, much of it with personal information about all of us, are probably beyond our individual comprehension. The ubiquity of the Internet is its strength, and the ubiquity of the Internet is its weakness. And we are all potentially exposed to the potential malignant use of the Internet and the nefarious use of our information that is on it.

I say to friends, lawyers, or non-lawyers, all of us have a role and a need to combat its improper use. Its misuse, even potentially by our own government, is a clear and, I think, ever-present danger. We can never take for granted that our government, acting on its own, has the capability to protect us from its destruc-

* Secretary of the Department of Homeland Security, 2003–05. This speech was delivered by Thomas J. Ridge at the 2016 *University of Richmond Law Review Symposium*, *National Security in the Information Age: Are We Heading Towards Big Brother*, on October 28, 2016, at the University of Richmond School of Law.

tive use. All of us interact with the Internet as users, consumers, and citizens. Most of us are unaware of the total amount of personal information the government and the commercial sector have about us.

We know the Chinese have the profiles of 22 million Americans after the Office of Personnel Management breach (in 2015), including mine. We were required to provide that information to government to serve our country. Understandable.

But add on top of that a layer of information that those 22 million—and, I might add, all of you—voluntarily surrender.

Do you have the slightest idea of the depth and breadth of information they have about you? I would dare say not, and I say this respectfully. On that "click consent," when you agree to the terms of service and privacy statement, how many of you have thoroughly read it and understand its implications? Do not raise your hand because you will be like the lone ranger, probably. It is not a criticism. I plead guilty.

When you automatically, and I think without hesitation, hit the "click consent" to the terms of service and privacy policy, you probably empower the ISP the right to accumulate and sell the following: things you search, websites you visit, videos you watch, ads you click on, your location information, IP address, and cookie data, and I suspect some missing other elements which could probably be described as "data exhaust."

Do you think that "click consent," law students, is tantamount to informed consent? Interesting question, isn't it? Could you function without ISP platforms in your personal or professional life? Let us not forget the information citizens share with organizations with whom they are associated, telecommunication companies, financial firms, health care providers—a pretty long list. Much of it is mandated, and unprecedented levels are volunteered and, yes, some surreptitiously acquired.

Now, I rarely applaud the United Nations, and particularly the United Nations Human Rights Council, but I have to admit it addressed the issue of privacy several years ago when it affirmed for the first time that human rights in the digital realm should be afforded the same protection as human rights in the physical world. One of the participants in the council meeting, Ambassador Hans

Schumacher of Germany, observed, "Every person is entitled to a private sphere, free from undue interference or surveillance by the state or by other actors." He urged the global community to strike a balance between legitimate public security concerns and the fundamental right to privacy in the digital age. We all know there are UN members who do not share that point of view. I happened to be in China talking about cybersecurity about a year and a half ago, and I assure you, they do not share that. But the United States does, and must, if our democracy is to remain the strongest and most respected expression of self-government in the world. The relationship between countries and their citizens on this matter varies dramatically. Rarely is there complete transparency of the government's role.

Governments, for legitimate reasons, have access to and retain personal information about its citizens.

But with the advent of Facebook, Twitter, LinkedIn, and so many social media alternatives, citizens living in the modern world surrender information about themselves with astonishing regularity and without hesitation. Think about this a moment: Devices used by the population every day can be used to determine where you are; you do have a GPS-enabled iPhone or iPad, don't you? Or what you are thinking—let us see what website you just clicked on. We take it for granted. It says a lot about each and every one of us.

Some or all of this information can be collected, sorted, analyzed, and used to profile and target individuals and groups through the digital networks for economic, social, national security, even political reasons. It is all out there, available for use or abuse.

The embrace of all that is digital—which means all that is accessible—may suggest that we Americans do not cherish our privacy. Be assured, we do. We must. Preserving our civil liberties and privacy was clearly a concern of the administration and Congress. In response to the attack of 9/11, the Department of Homeland Security was created and the first-ever congressionally mandated privacy office was included. The country believed then, it believes now, that no matter how effective the technology might be to identify terrorists before they strike—a worthy, laudable, and essential goal—no matter how grave the threat may be, pre-

serving civil liberties is itself an essential part of protecting the homeland.

The privacy office was built to look carefully at what was collected, how it should be stored, whether or not it could be collated, whether it contained personally identifiable information, how long the data could be held, and finally for what purpose it should be made available to the government.

In 2004, on the recommendation of the 9/11 Commission, a privacy and civil liberties oversight board was created and housed in the executive branch. Listen carefully to the following: Although President Bush submitted four names in 2008, the Senate took no action. President Obama made several nominations in 2010, but it took until August of 2012 for Congress to confirm them. This may surprise or it may disappoint you, but it was only earlier this year that a highly regarded technology adviser became part of that indispensable team.

This short history is troubling and very revealing. If we rely exclusively on government to monitor the use of technology and its impact on our privacy, I say, respectfully, our faith will be somewhat misplaced.

Attempts to create permanent and rigorous oversight capabilities within the government have certainly been well-intentioned, but that limited track record says they are feeble at best. We can only hope they improve. We must remind ourselves that technology moves more quickly than government. Then again, so do icebergs.

I recently read that the amount of stored information grows four times faster than the economy, while the processing power of computers has grown nine times faster. Authors Viktor Mayer-Schönberger and Kenneth Cukier concluded, "The real revolution is not in the machines, but in the data itself and how we use it." The analysis that big data has and will contribute to more efficient manufacturing, more productive agriculture, improved health care, safer transportation, a cleaner environment—the actual potential benefits are almost limitless.

We should and can celebrate the positives, but we cannot ignore the negative. The benefits are derived, in many instances, from using complicated math algorithms to make predictions.

When the analysis involves personal information and the possibility or probability of certain actions or certain kinds of behavior, I think government and society must proceed with caution.

Let me share with you both a personal example of predictive analysis and the concerns that I think we legitimately need to pay attention to. I gave a graduation speech at another law school, and one of the students who was the daughter of a friend of mine gave me four unidentified, untitled books as a present. Imagine that. It is an interesting gift certificate. I was asked to provide basic personal information about myself and then express—on one sheet of paper, fill-in-the-blanks, a couple questions—my literary tastes and the kinds of things that interest me. I have got a pretty wide range, so I put most of them down there.

The algorithm used by the company to select these books was amazingly—and I must admit, uncomfortably—accurate. They may not have been on my choices walking through Barnes & Noble, but the computer made superb choices for me. It does not take too great an imagination to foresee the potential abuse of personal information and predictive analysis if the capability is in the wrong hands. That capability exists in our world today.

We need not take a leap of faith into the future when government's misuse of its access to big data—surveillance cameras, sensors, supercomputers initially designed and offered to protect us from terrorist attacks—is used to undermine our democracy.

There must be rules circumscribing who has access to the data and how it is used. In the information age, pieces of digital DNA, our digital soul, are scattered everywhere. We must be vigilant that government never gathers the information that subjects us to the tyranny of the algorithm.

As you are aware, at least the law students here are aware, there is a series of Supreme Court opinions that affirm the notion that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties. Third party doctrine. I personally think it is time for policymakers to reconsider that notion. I think that blanket approach is ill-suited in the digital forevermore. I believe citizens should be able to control the use of their own personal information in the cyber age.

I think that is worthy of a national discussion that should include the tech giants of our world. They are the ones that gather the information, sell it, and have access to it through all sorts of captive audience. The belief that the most effective means of protecting our privacy and civil liberties is controlling the collection and storage of data is both obsolete and impossible. I have read estimates from 50 billion to 70 billion devices will be hooked on the Internet by 2025. I have no idea how that translates into the data that is going to be available. No idea. Nobody does. We are not going to put the data genie back in the bottle. It is exploding exponentially in the digital forevermore. It will continue to do so.

Limiting government's reach into the private domain of the citizen will be a permanent challenge in this digitally engaged, digitally promising, and potentially digitally dangerous world. Technology must surely be an instrument of government to combat threats regardless of their nature. Technology can never be a weapon against its citizens.

As we combat radical terrorism, as we confront social and political unrest, as we fight the never-ending battle against crime, there will be in the digital forevermore a permanent tension between safety, security, and privacy. Given the gigabytes of information that exist about people, places, and things, the surveillance and sensor systems that become more embedded in our community and our daily lives, we have to be mindful of not only the enabling use but the potential for misuse.

Here is where I strongly believe the professional and private voices of the legal profession must be heard. And I suspect, when you graduate from the University of Richmond Law School, you will be prepared to raise those voices. When it comes to protection of our privacy, I also hope and expect, in a certain prayerful way, that you do.