Privacy in the Digital Age: A Conversation with Michael Chertoff

SPEAKER:

Michael Chertoff, Co-Founder and Executive Chairman, Chertoff Group; Former Secretary of Homeland Security

INTERVIEWER:

David Lawrence, Founder and Chief Collaborative Officer, RANE

One of the most dangerous threats we face today is the increasingly pervasive exposure of our personal information. As we are ever more vulnerable to cyber-attack, we are also increasingly vulnerable to the loss of control of this information.

In his new book, Exploding Data: Reclaiming Our Cyber Security in the Digital Age*, former Secretary of Homeland Security Michael Chertoff argues that our laws and policies surrounding the protection of personal information need to be completely overhauled for the Internet era. Complex legal issues surround data collection and dissemination, and Chertoff maintains we need to rethink the balance between privacy and security for governments, businesses, and individuals.*

RANE Founder and Chief Collaborative Officer David Lawrence recently sat down for an in-depth, one-on-one conversation with Chertoff, founder of the Chertoff Group, to explore these issues. Highlights of the discussion follow.

THE CHALLENGE OF A BORDERLESS DIGITAL WORLD

The conversation began with **David Lawrence** asking **Michael Chertoff** if digital borders exist in today's world, which the former Secretary of Homeland Security answered clearly.

According to **Chertoff**, "There are no digital borders. I mean the whole idea of the internet is a network of networks that transcends physical borders. It means that, for example, it's not always clear what law applies to the data in question because the data moves around and isn't necessarily housed where the citizens are. It means that bad actors in other parts of the world can reach across the globe and attack us and be relatively immune from being caught and prosecuted because they're in a different country."

It is because of this daunting challenge that **Chertoff** said he wrote his new book, *Exploding Data: Reclaiming our Cyber Security in the Digital Age*. He wanted to "alert people to the fact that when they think about what they value, their privacy, their security and their freedom, they need to be at least just as concerned about what can be done by the private sector with the mountain of data that we generate as they should be about what the government can do."

He also wants those same people to be cognizant that individuals produce data (from their conversations or transactions online to their locations in the physical world) at a much higher volume than they realize. As part of this common (and potentially costly) misunderstanding, people often lose sight of how information exchanged on the internet is preserved forever.

Before the internet age, **Chertoff** noted, people "distinguished between what goes on in private, and what you do out on the street that's public. And the view was that with respect to things you do in public, you don't have any right to complain if people see it, record it, and do things with it because you're in public." Yet there was a widespread assumption that, unless one was famous, very few people would ever see what one did in public. He called this "information friction," a now extinct idea whereby "the ability to store and transmit and use [personal] information in public was inherently limited. And so, if you did something that was foolish, or you wanted to have forgotten, eventually, chances are, for most people, it would be."

Chertoff pointed out that the American judicial system is beginning to recognize how technology has "qualitatively changed" the rules, which is beneficial to privacy preservation.

CAN YOU EVER CONTROL YOUR DATA AGAIN?

Chertoff cited the recent Supreme Court case *Carpenter v. United States*, in which the government subpoenaed a day's worth of locational data for a cell phone from the target of an investigation.

He pointed out that the American judicial system is beginning to recognize how technology has "qualitatively changed" the rules, which is beneficial to privacy preservation; a search warrant must now be used to pull specific data from devices: "You're beginning to see the courts adapt the rules of the Fourth Amendment to the [ubiquity] of the new technology." However, given technology's unlimited storage capacities and ability to send information rapidly around the world, our fundamental understanding of what "public" means is changing, and embedded assumptions of how our privacy gets handled is shifting.

Chertoff's general thesis is the "idea that you can hide your data is really not realistic anymore because a lot of data is generated even by third parties without your knowledge or consent: People who record you or take a picture of you and post it on Facebook or tell somebody else or record what is said." The questions that **Chertoff** seeks to address in Exploding Data is not necessarily about hiding data—rather, it focuses on "Can you control it even after it's out there? Do you have a right to have a say in whether it's resold or whether it's used to target you for certain behavioral purposes?"

UNDERSTANDING HOW YOUR DATA IS BEING (MIS)USED

Chertoff brought up online waiver forms (for such things as terms of service) to highlight most individuals' understandable ignorance of how their data is really being used. There are three elements to these forms that hamper consumers' ability to know where their information is headed: "One is, of course, they're famously long, full of legal jargon and virtually not understandable to an average mortal even if that person has the patience to read it. But there are really two other deeper problems. When you consent to broad use of your data you don't necessarily do it with an understanding of all the other data you have out there, and the fact that it may be combined so that someone or some enterprise may have a picture of all of your data streams."

HOW COMPANIES VIEW DATA

Chertoff agreed with **Lawrence** that the business model for most companies is less about advertising and more about data aggregation. He calls data "the new gold," describing that its high value stems from its ability, combined with the field of data analytics, to "allow people to create all kinds of services or products. Whether it's advertising, whether it's political campaigning, whether it's road testing certain kinds of products, all kinds of things flow from the data." **Chertoff** believes that people have "finally begun waking up" to the idea that the consumer is "actually the product."

CYBER THREATS IN THE PUBLIC ARENA

While the private sector may be particularly vulnerable to cyber threats because it is the venue for the bulk of "digital activity," **Chertoff** stressed that the public sector and arena is also a vulnerable target, especially with regards to voting and elections. He believes that the Department of Homeland Security is doing what it can to address the problem, "teaching them how to upgrade some of their protections for the databases and the data itself while making sure an audit trail is generated…so you can always go back and verify that no one has done anything to corrupt or interfere with the voting process."

While the private sector may be particularly vulnerable to cyber threats because it is the venue for the bulk of "digital activity," Chertoff stressed that the public sector and arena is also a vulnerable target, especially with regards to voting and elections.

Chertoff continued on the subject of democracy-related concerns, covering two different issues that arise "because of what used to be called propaganda and is now called information operations, which is the effort by the Russians and even other countries to manipulate the media in order to drive social discord and try to affect behavior." He pointed out that automated processes, or "bot nets," can deliberately mislead people, generating falsified reports, creating fake profiles, and driving up the number of "likes" on a posting, for instance. **Chertoff** believes that companies are now getting serious about eliminating these issues from platforms, but that there is still much to be done with regard to informing people and countering the threat. While the First Amendment must be protected, he asserted, foreign governments do not have any rights to mislead the American public as they have been doing of late.

THE ROLES OF GOVERNMENT IN DATA PRIVACY

Chertoff lamented that in the early days of the internet, there was resistance to government involvement, that some activists would say that the internet "is all for good. It's freedom. It's innovation. Let's not get the clunky government involved, this is all about cutting edge technology." However, there were real downsides, and as technology further develops, he emphasizes the importance of ensuring that the government protects people against those downsides.

When **Lawrence** asked about an inherent distrust between the general population and government when it comes to data privacy and internet regulation, **Chertoff** countered that in Europe "it's kind of the reverse. In Europe, there's a lot of skepticism about the private sector. Their privacy rules tend to be much more focused on the private sector. And they're actually somewhat more trusting of government." He praised the European approach, explaining that regulations there "do give citizens some say in the use of data even after it's been collected by an enterprise," and speculated that US data privacy laws may one day follow the European example.

Chertoff added that he does "understand why, traditionally, Americans are nervous about government." He said that the US Government, in the "understandable interest of protecting classified information," has a tendency to be "opaque" when it comes to making

publicly available how data is processed. He recommends that the government should be more transparent "as a way of reassuring people that, for the most part, the government is really quite scrupulous — because they get punished otherwise — about obeying the laws."

Chertoff said that the US Government, in the "understandable interest of protecting classified information," has a tendency to be "opaque" when it comes to making publicly available how data is processed.

Chertoff believes that some of these changes could "be done by congress, legislating, and whether it would be the Federal Trade Commission or the Federal Communications Commission, giving a regulatory agency some authority to actually get into prescribing with greater level of detail what your obligations are with respect to giving people insight into the use of their data." However, he argued that grassroots, state-level initiatives may be most effective and expedient, and that incrementally, corporations will begin to change their data privacy policies: "California just passed a law. I think it comes into effect in about 18 months. That again gives people some control over their data and as much the same way as you see in the environmental area, it may be that a number of states take the lead in setting up rules that will in effect be nationalized because if you're a major enterprise, and you're operating in 50 states and California and New York have certain requirements, you're going to have to comply with those, and it probably makes sense to do it on a nationwide basis."

This may also eventually be the case globally, with Europe's new General Data Protection Regulation (GDPR) becoming the de facto standard that multinational companies have to follow. As **Chertoff** put it, "If you're a global enterprise and you're complying with European requirements on control of data, it may be easier just to make it a global requirement."

ABOUT THE EXPERTS

Michael Chertoff, Co-Founder and Executive Chairman, Chertoff Group

As Secretary of the U.S. Department of Homeland Security from 2005 to 2009, Michael Chertoff led the country in blocking would-be terrorists from crossing our borders or implementing their plans if they were already in the country. Chertoff also transformed FEMA into an effective organization following Hurricane Katrina. At Chertoff Group, he provides high-level strategic counsel to corporate and government leaders on a broad range of security issues, from risk identification and prevention to preparedness, response and recovery. Before heading up the Department of Homeland Security, Chertoff served as a federal judge on the U.S. Court of Appeals for the Third Circuit, as well as a federal prosecutor. Chertoff is also senior of counsel at Covington & Burling LLP, and a member of the firm's White Collar Defense and Investigations practice group.

David Lawrence, Founder and Chief Collaborative Officer, RANE

Before launching RANE, David Lawrence previously served for approximately 20 years as Associate General Counsel and Managing Director at Goldman Sachs. During his tenure, Lawrence formed and was the global head of the Business Intelligence Group, covering a wide range of legal, regulatory, diligence and transactional responsibilities for the firm, as well as advising Goldman's clients directly. Prior to working at Goldman Sachs, Lawrence was for 10 years an Assistant US Attorney, in the Southern District of New York, where his roles included Deputy Chief of the Criminal Division and Chief of the Public Corruption and General Crimes Units.

ABOUT RANE

RANE (Risk Assistance Network + Exchange) is an information and advisory services company that connects business leaders to critical risk insights and expertise, enabling risk and security professionals to more efficiently address their most pressing challenges and drive better risk management outcomes. RANE clients receive access to a global network of credentialed risk experts, curated network intelligence, risk news monitoring, in-house analysts and subject matter experts, and collaborative knowledge-sharing events.