Chambers

GLOBAL PRACTICE GUIDES

Definitive global law guides offering comparative analysis from top-ranked lawyers

Cybersecurity

Introduction
Alan Charles Raul
Sidley Austin LLP

practiceguides.chambers.com

2021

INTRODUCTION

Contributed by: *Alan Charles Raul,* ***Sidley Austin LLP***

A New Paradigm for Cybersecurity Defence: Strategy, Leadership, Diplomacy and Guidance

The Cyberspace Solarium Commission, a high-level, bipartisan group established by the US Congress, attributed the weakness of the nation's cybersecurity posture to failures of strategy and leadership. There could hardly be a more damning indictment of government failure or a clearer explanation for why national security and economic prosperity are so threatened by the risk of cyber-attack, theft and compromise. And what is sadly true of the United States of America on this score is no less true among other democratic, developed countries. This must change if cyber past is not to be prologue regarding future cyber-insecurity.

Government accountability and engagement are key to meaningful progress. The new administration in Washington is legislatively mandated to appoint a senior cybersecurity official in the White House, and to enhance the Cybersecurity and Infrastructure Security Agency. But much more must be done.

It is critical that like-minded countries establish a multilateral process to address material privacy and economic cybersecurity risks, akin to the efforts of the global community to tackle climate change.

Governments must take responsibility for protecting their domestic information networks – very much including the private sector – and the sensitive personal information of their citizens. It is ironic how much attention is accorded, in particular by European countries and non-governmental organisations, to the risks to privacy of corporate acquisition of consumer data for advertising purposes versus how little attention is paid to the wide-scale compromise and theft of acutely sensitive private information by malicious state actors and global cybercriminals.

While cybersecurity will always entail a public-private sector "partnership," governments must be held responsible – and politically accountable – for protecting the private sector. It is axiomatic in cybersecurity circles that organisations must "be right" 999 out of 1000 times – ie, essentially perfect – to defend themselves against sophisticated threat actors. But as Vice President Kamala Harris acknowledged while serving as California Attorney General in 2016, and as the Federal Trade Commission routinely concedes, there is no such possibility of perfect information security.

Accordingly, pursuing enforcement action against companies that inevitably fail to be perfect, or allowing private litigants to demand perfection of entities that experience a data breach (including numerous government agencies), is not as helpful an incentive as one would imagine. Hiring the best talent and spending enormous amounts on information security is no guarantee either.

Given this reality, governments must establish a new paradigm for cyberprotection. There ought to be much more strenuous government defensive, offensive and diplomatic measures to deter, prevent and punish malicious state actors and global cybercriminals. This must be undertaken on a co-ordinated basis at the highest levels of government (ie, no lower than ministerial).

For the private sector, governments should develop agreed standards and guidance for what constitutes "reasonable security" for organisations depending on their size, sensitivity of systems and data, and role in the cyber "supply chain." Governments should also promote and encourage the development of attestation models and structures on which companies may rely for their self-assessments of "reasonable security."

At present, the only real consensus is that cybersecurity risks are growing and that current approaches are not working (or at least not nearly well enough). The world's governments must do (much) better.

Sidley Austin LLP is a global law firm with 2,000 lawyers in 20 offices around the world. The firm's privacy and cybersecurity group has more than 70 professionals across offices in the USA, London, Brussels, Geneva, Hong Kong, Singapore and Tokyo. Sidley Austin represents clients in a broad range of sectors, including financial services, life sciences and healthcare, tech, communications and media, information service providers, professional services and internet companies. The firm undertakes highly sophisticated legal counselling and advocacy, and provides actionable legal advice on challenging and novel questions of privacy and information law. Sidley's lawyers focus on privacy, data protection, information security, digital governance, internet and computer law, e-commerce, consumer protection, outsourcing, competitive intelligence and trade secrets, information management and records retention, and responding to cybercrimes and network intrusions. The team also handles litigation and government investigations; crisis management and incident response; compliance and regulatory counselling on all data protection laws, such as GDPR and CCPA; legislative and policy developments; and international data transfers.

Contributing Editor

Alan Charles Raul is a partner and the founder and leader of Sidley's privacy and cybersecurity practice. He represents companies on federal, state and international privacy, cybersecurity and digital technology issues. His practice covers global data protection and compliance programmes, data breaches, crisis management, consumer protection issues and internet law. Alan advises companies on cybersecurity preparedness and digital governance, and on litigation, regulatory defence, internal investigations, and policy advocacy. He handles consumer class actions, enforcement matters and public policy involving the FTC, State Attorneys General, the SEC, the FCC, the DOJ, international data protection authorities and other government agencies. Alan is a member of the American Bar Association's Cybersecurity Legal Task Force, the Technology Litigation Advisory Committee of the US Chamber Litigation Center, the PLI's Privacy Law Advisors Group, the Council on Foreign Relations, and the governing Board of Directors of the Future of Privacy Forum.

Sidley Austin LLP

1501 K Street, N.W.
Washington
DC 20005

Tel: +1 202 736 8477
Email: araul@sidley.com
Web: www.sidley.com

SIDLEY