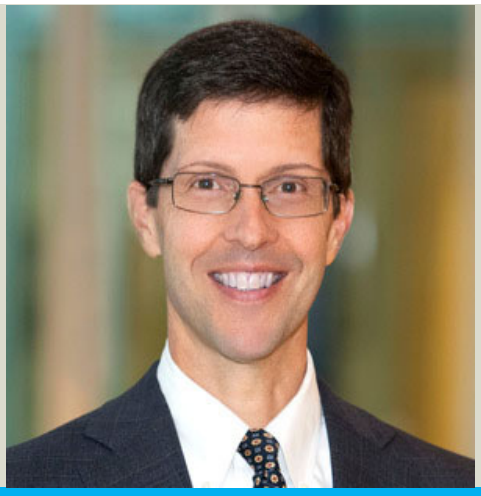

William R. Denny

Privacy and Cyber Risks in the Connected World: Connected Cars and Medical Devices

The explosion of connected devices in our society, from toasters, refrigerators and doorbells to wearable devices, cell phones and even our cars, has changed the nature of the risks we face and led to data being collected in ways we could not imagine only a few years ago. This creates new attack surfaces that make them vulnerable to cyber-attack. I will focus on privacy, cybersecurity, and data ownership concerns through two use cases: connected cars and connected health care devices.

Biography

Mr. Denny is a partner at Potter Anderson & Corroon LLP in Wilmington, Delaware, where he leads the practice area of cybersecurity, data privacy and information governance. Bill is a Certified Information Privacy Professional (CIPP/US) and a Certified Information Privacy Manager (CIPM) through the International Association of Privacy Professionals (IAPP). He has represented public and privately held companies and government entities in a wide range of technology transactions, including negotiating complex cloud services agreements, software and IT infrastructure development, maintenance and support agreements, long-term materials supply agreements, outsourcing agreements, transition and site services agreements, technology licensing agreements, sales of internet domain names, and website terms of use and privacy policies. Clients include major corporations in the industrial, chemical, medical and technology sectors, as well as technology and information systems service providers and developers.

Bill has litigated disputes over the interpretation and enforcement of many types of technology contracts, general commercial contracts and liability insurance policies. He has tried jury and non-jury cases in federal and state trial and appellate courts, before arbitration panels, and by use of other alternative dispute resolution techniques. Bill took a leading role in drafting and negotiating Delaware's amendment to its computer security breach law, 6 Del. C. §§ 12B-100 et seq., which was enacted in June 2017 and came into force in April 2018.