INFORM. INSPIRE. DEVELOP CIVIC LEADERS.

THE POLICY CIRCLE

DATA PRIVACY & CYBERSECURITY

WHAT IS DATA PRIVACY & CYBERSECURITY?

DATA PRIVACY EMPOWERS CITIZENS TO MAKE THEIR OWN DECISIONS ABOUT WHO CAN PROCESS THEIR DATA AND FOR WHAT PURPOSE

CYBERSECURITY IS THE PRACTICE OF PROTECTING SYSTEMS, NETWORKS, AND PROGRAMS FROM DIGITAL ATTACKS. THESE CYBERATTACKS ARE USUALLY AIMED AT ACCESSING, CHANGING, OR DESTROYING SENSITIVE INFORMATION; EXTORTING MONEY FROM USERS; OR INTERRUPTING NORMAL BUSINESS PROCESSES.

FACTS TO KNOW

72% OF AMERICANS BELIEVE MOST OF THEIR ONLINE ACTIONS ON THEIR PHONES AND COMPUTERS ARE TRACKED BY ADVERTISERS AND TECH FIRMS, AND 80% DO NOT BELIEVE THEY HAVE CONTROL OVER DATA COLLECTED ABOUT THEM.

THE MARKET FOR GLOBAL DATA PROTECTION AND CYBERSECURITY AS A SERVICE IS EXPECTED TO INCREASE FROM $7.6 BILLION IN 2017 TO $28.2 BILLION BY 2023. THE MARKET FOR BIG DATA, DATA ANALYTICS, AND CLOUD SERVICES IN GENERAL WAS MEASURED AT JUST UNDER $5 BILLION IN 2018 AND IS EXPECTED TO REACH $61.42 BILLION BY 2026.

THE HEALTHCARE INDUSTRY SUFFERED MORE CYBERSECURITY BREACHES THAN ANY OTHER INDUSTRY IN 2018 AND 2019. THERE WERE 510 HEALTHCARE DATA BREACHES OF 500 OR MORE RECORDS IN 2019; IN TOTAL, IT IS ESTIMATED THAT HEALTHCARE RECORDS OF OVER 12% OF THE U.S. POPULATION WERE BREACHED. IN THE FIRST SIX MONTHS OF 2020, THERE WERE 224 HEALTHCARE DATA BREACHES OF 500 OR MORE RECORDS. OVER 9 MILLION RECORDS WERE EXPOSED IN SEPTEMBER 2020 ALONE AS A RESULT OF A MAY 2020 RANSOMWARE ATTACK ON CLOUD SOFTWARE COMPANY, WHICH AFFECTED AT LEAST 80 HEALTHCARE ORGANIZATIONS.

FROM JANUARY TO AUGUST OF 2018, 103 FINANCIAL SECTOR BREACHES WERE REPORTED (AMOUNTING TO ALMOST $17 BILLION), COMPARED TO 37 BREACHES IN 2016. THE CAPITAL ONE DATA BREACH IN JULY 2019 EXPOSED THE DATA OF OVER 100 MILLION PEOPLE IN THE UNITED STATES AND CANADA, INCLUDING 140,000 SOCIAL SECURITY NUMBERS, 1 MILLION SOCIAL INSURANCE NUMBERS (THE CANADIAN EQUIVALENT OF SOCIAL SECURITY) AND 80,000 BANK ACCOUNT NUMBERS.

GOVERNMENT EXPENDITURES

THE FEDERAL GOVERNMENT SPENT OVER $18 BILLION ON CYBERSECURITY IN FY2021. ABOUT 87% OF LOCAL GOVERNMENTS PROVIDE CYBERSECURITY TRAINING FOR EMPLOYEES, BUT ONLY 56% OF THOSE PROVIDE ONGOING TRAINING AND 33% PROVIDE TRAINING ONLY ONCE A YEAR.

THE 2020 NATIONAL SURVEY OF LOCAL GOVERNMENT CYBERSECURITY PROGRAMS FROM THE PUBLIC TECHNOLOGY INSTITUTE, FEWER THAN 25% OF IT EXECUTIVES SAY THEIR ELECTED OFFICIALS ARE ACTIVELY ENGAGED IN THEIR GOVERNMENT'S CYBER EFFORTS, AND 66% SAY THEY DO NOT BELIEVE THEIR CYBERSECURITY BUDGET IS ADEQUATE.

Table 24–1. AGENCY CYBERSECURITY FUNDING TOTALS
(In millions of dollars)

	FY 2018	FY 2019	FY 2020
Department of Agriculture	262	480	311
Department of Commerce	350	403	392
Department of Defense	8,048	8,734	9,643
Department of Education	104	139	143
Department of Energy	448	520	557
Department of Health & Human Services	359	474	460
Department of Homeland Security	1,859	1,921	1,919
Department of Housing & Urban Development	15	35	25
Department of Justice	821	824	881
Department of Labor	93	93	94
Department of State	362	363	400
Department of the Interior	88	103	111
Department of the Treasury	445	505	522
Department of Transportation	185	224	232
Department of Veterans Affairs	386	530	513
Environmental Protection Agency	21	44	45
General Services Administration	72	79	80
National Aeronautics & Space Administration	171	169	171
National Science Foundation	247	239	224
Nuclear Regulatory Commission	25	32	29
Office of Personnel Management	38	45	47
Small Business Administration	9	16	16
Social Security Administration	167	225	205
U.S. Agency for International Development	44	68	44
Non-CFO Act Agencies	362	382	372
Total	**14,978**	**16,645**	**17,435**

FRAMING THE ISSUE

THE U.S. CONSTITUTION PROTECTS INDIVIDUAL PRIVACY FROM GOVERNMENT INTRUSION, BUT DOES LITTLE TO PROTECT THAT PRIVACY FROM ACTORS OUTSIDE THE GOVERNMENT. THIS APPLIES TO DATA AS WELL. DATA LAWS PROVIDE “INDIVIDUALS WITH RIGHTS OVER THEIR DATA, IMPOSING RULES ON THE WAY IN WHICH COMPANIES AND GOVERNMENTS USE DATA, AND ESTABLISHING REGULATORS TO ENFORCE THE LAWS.”

BUSINESSES AND SERVICES RELY ON ANALYTICS COMING FROM DATA SHARING, DATA TRACKING, AND EVEN ARTIFICIAL INTELLIGENCE. THE DEVICES WE CARRY WITH US AND INSTALL IN OUR HOMES ALL GENERATE DATA. THESE NEW WAYS OF USING TECHNOLOGY REQUIRE NEW WAYS OF THINKING ABOUT AND PROTECTING DATA. A LACK OF DATA PRIVACY AND PROTECTION OPENS THE DOOR FOR DANGEROUS ACTORS TO TAKE ADVANTAGE OF DIGITAL VULNERABILITIES.

AT THE STATE LEVEL, IT IS MUCH EASIER TO PASS DATA PRIVACY LAWS, AND EASIER FOR ATTORNEYS GENERAL TO ENFORCE CONSUMER PROTECTION LAWS. AT THE SAME TIME, THERE BEING NO SINGLE LAW THAT REGULATES CONSUMER PROTECTION IN DATA COLLECTION CREATES A PATCHWORK OF LAWS.

IN DECEMBER 2020, A MASSIVE DATA BREACH LINKED TO THE TEXAS-BASED SOFTWARE COMPANY SOLARWINDS WAS REPORTED. HACKERS SPENT MONTHS INSIDE U.S. GOVERNMENT NETWORKS; AFFECTED FEDERAL AGENCIES INCLUDED THE COMMERCE DEPARTMENT, THE DEPARTMENT OF HOMELAND SECURITY, THE PENTAGON, THE TREASURY DEPARTMENT, THE U.S. POSTAL SERVICE, AND THE NATIONAL INSTITUTES OF HEALTH. SUCH HACKING RAISES THE QUESTION OF WHAT NATIONAL SECURITY LOOKS LIKE IN THE DIGITAL AGE.

SOLUTIONS

THE MOST INFLUENTIAL PRIVACY LAW OVERSEEING DATA-COLLECTION IS CALIFORNIA'S CONSUMER PRIVACY ACT, PASSED IN JUNE 2018 AND IN EFFECT AS OF JANUARY 1, 2020. NEVADA AND MAINE HAVE FOLLOWED SUIT, PASSING THEIR OWN PERSONAL DATA PROTECTION LAWS, AND STATES FROM WASHINGTON TO OKLAHOMA TO FLORIDA ARE PUSHING AHEAD WITH DATA PROTECTION LEGISLATION AS OF EARLY 2021. A NUMBER OF STATES INCLUDING NEW YORK, NEW JERSEY, MARYLAND, OREGON, AND TEXAS HAVE ALSO PASSED DATA BREACH NOTIFICATION LAWS.

MANY BELIEVE THESE STATE ENDEAVORS,COULD BE THE TURNING POINT THAT SPURS LAWMAKERS INTO ACTION TO CREATE A NATIONAL LAW FOR DATA PRIVACY AND SECURITY, SIMILAR TO THE EUROPEAN UNION'S GENERAL DATA PROTECTION REGULATION. MANY BELIEVE IT SHOULD FOCUS ON PROTECTING THE PERSONAL DATA OF EVERYDAY CITIZENS; PROVIDING CONSUMERS WITH TRANSPARENCY AND CONTROL; AND ENSURING PROPER GOVERNANCE AND ENFORCEMENT OF SAFETY MEASURES. IN DOING SO, IT WOULD: CHAMPION CONSUMER PRIVACY AND PROMOTE ACCOUNTABILITY TO ENHANCE CUSTOMER TRUST; FOSTER INNOVATION AND COMPETITIVENESS TO DEMONSTRATE U.S. LEADERSHIP IN THE REALM OF PRIVACY FOR THE PURPOSE OF INNOVATION AND ECONOMIC COMPETITIVENESS; HARMONIZE REGULATIONS TO ELIMINATE THE EXISTING PATCHWORK SYSTEM; ACHIEVE GLOBAL INTEROPERABILITY TO COOPERATE WITH THE INTERNATIONAL ECONOMY AND E-COMMERCE TRANSFERS OF PERSONAL DATA.

WHAT YOU CAN DO

FIND OUT WHAT YOUR LOCAL AND STATE GOVERNMENT INSTITUTIONS ARE DOING TO PROTECT YOUR DATA.

FIND HOW YOUR HEALTH DATA IS PROTECTED AND SHARED.

CONSIDER YOUR DATA PROTECTION AND PRACTICES AT HOME AND AT WORK. TAKE A LOOK AT THIS DATA DETOX KIT FOR IDEAS.

REVIEW THE LIST OF LEGISLATION PRESENTED ABOVE AND INVITE YOUR REPRESENTATIVES IN CONGRESS TO DISCUSS THEIR POSITION ON THE TOPIC WITH YOUR POLICY CIRCLE. BY VOICING YOUR INTEREST, YOU DRAW THEIR ATTENTION TO THE TOPIC.