UNITED STATES PRIVACY REGULATIONS

General Overview

Privacy laws in the United States are constantly changing, especially as pandemic-related privacy breaches and data leakages become more frequent. We've provided brief overviews of several key privacy laws below to help you stay informed and recognize possible compliance issues.

BDO DIGITAL

COVID-19 DATA PRIVACY BILL

On May 7, 2020, U.S. Senator, Roger Wicker, chairman of the Senate Committee on Commerce, Science, and Transportation, along with U.S. Sens, John Thune, Deb Fischer, Jerry Moran, and Marsha Blackburn, introduced the COVID-19 Consumer Data Protection Act. The legislation provides all Americans with more transparency, choice, and control over the collection and use of their personal health, device, geolocation, and proximity data. Additionally, this Bill holds businesses accountable to consumers if they misuse personal data.

The COVID-19 Consumer Data Protection Act would:

- Require FTC regulated companies to obtain express consent to handle or collect personal health and geolocation information.
- Require companies not to disclose or transfer the data of individuals except as provided by the Bill.
- Direct companies to disclose to the consumer, upon collection, how the data is used, transferred, and how long it will be retained.
- Clearly define aggregate and de-identified data and adopt security protocols and technologies that prevent consumer data from re-identification.
- Establish mandatory consumer opt-out practices.
- Publish a data transparency report for the general public regarding data activities related to COVID-19.
- Require companies to adopt data minimization and security practices for Personally Identifiable Information (PII) collected by covered entities.
- Mandate companies to delete or de-identify all PII once the public health emergency has ended.
- Grant state attorneys general the right to enforce this legislation.

PUBLIC HEALTH EMERGENCY PRIVACY ACT

On May 14, 2020, both the House and Senate introduced the Public Health Emergency Privacy Act. Much like the COVID-19 Consumer Data Protection Act, this Act would put temporary rules in place regarding the collection, use, and disclosure of emergency health data used to combat the spread of the coronavirus.

The rules imposed by the Act would only apply during the Public Health Emergency as declared by the Secretary of Health and Human Services and would be limited to specific uses of certain personal data.

The law is an emergency measure to shore up privacy rights and risk mitigation in response to the COVID-19 pandemic, as organizations and government increasingly turn to processing personal information as a component of critical health and safety efforts like contact tracing.

The law requires:

- Purpose specification for data collected and used as a part of the health and safety pandemic response effort.
- Expressly prohibiting the use of personal information for privacy invasive means such as advertising.
- Limiting which public organizations/agencies process this health information and restricting access to those groups.
- Requiring data minimization practices.
- Prohibiting any penalties (such as voting restrictions) being placed on individuals who reject consent to participate in contact tracing efforts.
- Requiring analysis and reporting on the impact of these technologies and tools on data privacy.
- Mandating transparency in data processing.
- Ensuring an opt-in for data processing.

EXPOSURE NOTIFICATION PRIVACY ACT

On June 1, 2020, Senators Maria Cantwell and Bill Cassidy introduced the Exposure Notification Privacy Act (ENPA). The Act requires businesses that provide automatic notification of exposure to infectious diseases such as COVID-19 to include voluntary consent for enrollment and data privacy. Automated exposure notification service is defined as a tool for "digitally notifying in an automated manner, an individual who may have become exposed to an infectious disease." The ENPA covers information linked to any individual or device collected, processed, or transferred as part of an automated exposure notification service.[1]

The rules imposed by the Act apply to persons/entities covered by the FTC Regulation, nonprofit organizations, and common carriers as defined by the Communications act of 1934 (e.g., phone companies, broadcast stations, television, Internet, etc.). Additionally, the Act prohibits the discrimination of individuals based on their PII and the ENPA does not supersede or preempt State laws.

The law requires covered entities to:

- Not disclose or transfer the data of individuals except as provided by the Act.
- Publish privacy policies which provide notice of the type of data collected, purpose of collection, use of the data, and individual rights.
- Obtain the affirmative express consent of individuals before collecting their information.
- Provide individuals with the right to opt out of collection of their data and withdraw consent.
- Delete the individuals' data upon request or on a 30-day rolling basis.
- Safeguard the data of individuals through appropriate security measures.

CONTACT TRACING

On April 22, 2020, U.S. Senator Edward J. Markey issued recommendations to then Vice President Pence on protecting civil liberties and privacy rights. These recommendations address the United States' COVID-19 national contact tracing program.

The letter outlined that the program should:

- Be integrated with a comprehensive public health strategy that is designed to meet specific COVID-19 objectives.
- Involve the input of public health professionals and allows for the testing of effectiveness.
- Have a substantial workforce to aid in contact tracing.
- Include voluntary participation and be absent of any coercion.
- Provide data transparency to the end-user that provides clear and comprehensible information about the data collected including:
  - How data will be used.
  - Where data will be stored.
  - When data will be deleted.
  - How data will be protected.
  - Make all information readily available and open for inspection.
- Minimize data collection to only necessary information and limit its retention period.
- Restrict data use for COVID-19 purposes only and avoid collecting data that results in discriminatory outcomes.
- Implement the necessary safeguards to protect this data.
- Be applied equitably and include subpopulations.
- Be subject to enforcement and penalties for violations and misuse and allows for legal recourse.

1 "Tracing Papers": A Comparison of COVID-19 Data Privacy Bills

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES DISCRETION OF HIPAA PRIVACY AND SECURITY ENFORCEMENT

On March 17, 2020, the U.S. Department of Health and Human Services, Office of Civil Rights (OCR), released the "Notification of Enforcement Discretion for Telehealth Remote Communications During the COVID-19 Nationwide Public Health Emergency." Under the Notice, covered health care providers may use popular applications that allow for video chats, including Apple FaceTime, Facebook Messenger video chat, Google Hangouts video, etc., to provide telehealth, without risk that OCR might seek to impose a penalty for noncompliance with the HIPAA Privacy and Security Rules as long as such service is related to the good faith provision of telehealth during the COVID-19 nationwide public health emergency.

On April 9, 2020, the OCR announced that it will exercise enforcement discretion and will not impose penalties for violations of the HIPAA Privacy and Security Rules against covered entities or business associates in connection with the good faith participation in the operation of COVID-19 testing sites during the COVID-19 nationwide public health emergency.

On January 19, 2021, the OCR released the "Notification of Enforcement Discretion for Use of Online Web Based Scheduling Applications Scheduling COVID-19 Vaccination Appointments." Under the Notice, the OCR will not impose penalties for violations of HIPPA rules on healthcare providers and their business associates in connection with the good faith use of online and web based scheduling applications for the scheduling of individual appointments for COVID-19 vaccinations during the nationwide public health emergency. The announcement is effective as of the date announced with a retroactive effective date of December 11, 2020. The OCR encourages the use of minimum necessary Protected Health Information (PHI), encryption technology, and enabled privacy settings.[2]

PROMOTING DIGITAL PRIVACY TECHNOLOGIES ACT

On December 8, 2020, Representatives Haley Stevens and Anthony Gonzalez, Senators Catherine Cortez and Deb Fischer introduced the Promoting Digital Privacy Technologies Act (PDPTA) which would "support research on privacy enhancing technologies and promote responsible data use, and for other purposes."[3] The purpose of the Act is to ensure that data anonymization tools and privacy enhancing technologies (PETs) secure the personal data of individuals. The Act defines personal data as "information that identifies, is linked to, or is reasonably linkable to an individual or a consumer device, including derived data," and PETs are defined as "any software solution, technical processes, or other technological means of enhancing the privacy and confidentiality of an individual's personal data in data or data sets of data and includes anonymization techniques, filtering tools, anti- tracking technology, differential privacy tools, synthetic privacy data, and secure multi-party commutation."[4]

The PDPTA will require the National Science Foundation (NSF) to collaborate with the National Institute of Standards and Technology (NIST) to support research into PETs and work with academic, private, and public sectors including the National Institute of Health (NIH) and the Centers for Disease Control (CDC) to increase accountability in public health research. The Act also requires reports to Congress every two (2) years on progress with research and standard setting.

2 https://www.hhs.gov/about/news/2021/01/19/ocr-announces-notification-enforcement-discretion-use-online-web-based-scheduling-applications-scheduling-covid-19-vaccination-appointments.html

3 S.4981-116th Congress (2019-2020)

4 S.4981 Section 2 Definitions

CHILDREN'S ONLINE PRIVACY PROTECTION ACT

The Children's Online Privacy Protection Act (COPPA) imposes certain requirements on operators of websites or online services directed to children under 13 years of age, and on operators of other websites or online services that have actual knowledge that they are collecting personal information online from a child under 13 years of age.

The Act applies to websites or online services that have actual knowledge that they are collecting personal information directly from users of another website or online service directed to children. Operators covered by the Act must:

- Post a clear and comprehensive online privacy policy describing their information practices for personal information collected online from children.
- Provide direct notice to parents and obtain verifiable parental consent, with limited exceptions, before collecting personal information online from children.
- Give parents the choice of consenting to the operator's collection and internal use of a child's information, but prohibiting the operator from disclosing that information to third parties (unless disclosure is integral to the site or service, in which case, this must be made clear to parents).
- Provide parents access to their child's personal information to review and/or have the information deleted.
- Give parents the opportunity to prevent further use or online collection of a child's personal information.
- Maintain the confidentiality, security, and integrity of information they collect from children, including taking reasonable steps to release such information only to parties capable of maintaining its confidentiality and security.
- Retain personal information collected online from a child for only as long as is necessary to fulfill the purpose for which it was collected and delete the information using reasonable measures to protect against its unauthorized access or use.
- Not condition a child's participation in an online activity on the child providing more information that is necessary to participate in that activity.

On March 12, 2019 and July 23, 2019, Senator Ed Markey and Representative Bobby L. Rush introduced an amendment to COPPA, to strengthen protections relating to the online collection, use, and disclosure of personal information of children and minors, and for other purposes.

The amendment prohibits an operator of a website, online service, online application, or mobile application directed to a child or minor with constructive knowledge the user is a child or minor from collecting the user's personal information without:

- Providing notice and obtaining consent.
- Providing a parent or minor with certain information upon request.
- Conditioning participation by a user on the provision of personal information.
- Establishing and maintaining reasonable procedures to protect the personal information collected from users.
- The amendment prohibits targeted marketing directed to a child or minor without their consent and the sale of interconnected devices targeted to children and minors unless they meet certain cybersecurity and data security standards. The amendment further directs manufacturers of such devices to display a privacy dashboard that provides how personal information is collected and used.
- A parent or minor can challenge the accuracy of the personal information of the minor collected, and the operator must provide for the erasure or correction of the inaccurate information.[5]

5 H.R. 3900; S.78 – 116th Congress (2019-2020)

CONTROLLING THE ASSAULT OF NON-SOLICITED PORNOGRAPHY AND MARKETING ACT

The Controlling the Assault of Non0Solicited Pornography and Marketing Act (CAN-SPAM) controls commercial email while giving consumers the right to op-out and requires the Federal Trade Commission (FTC) to enforce its provisions. The CAN-SPAM Act sets the rules for commercial email, establishing requirements for commercial messages, and gives recipients the right to have emails stopped.

The CAN-SPAM Act doesn't apply only to bulk email, it covers all commercial messages, which the law defines as "any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service," including email that promotes content on commercial websites. The law makes no exception for business-to-business email.

This means all email – for example, a message to former customers announcing a new product line – must comply with the law.

Each separate email in violation of the CAN-SPAM Act is subject to penalties of up to $42,530.

CAN-SPAM's main requirements:

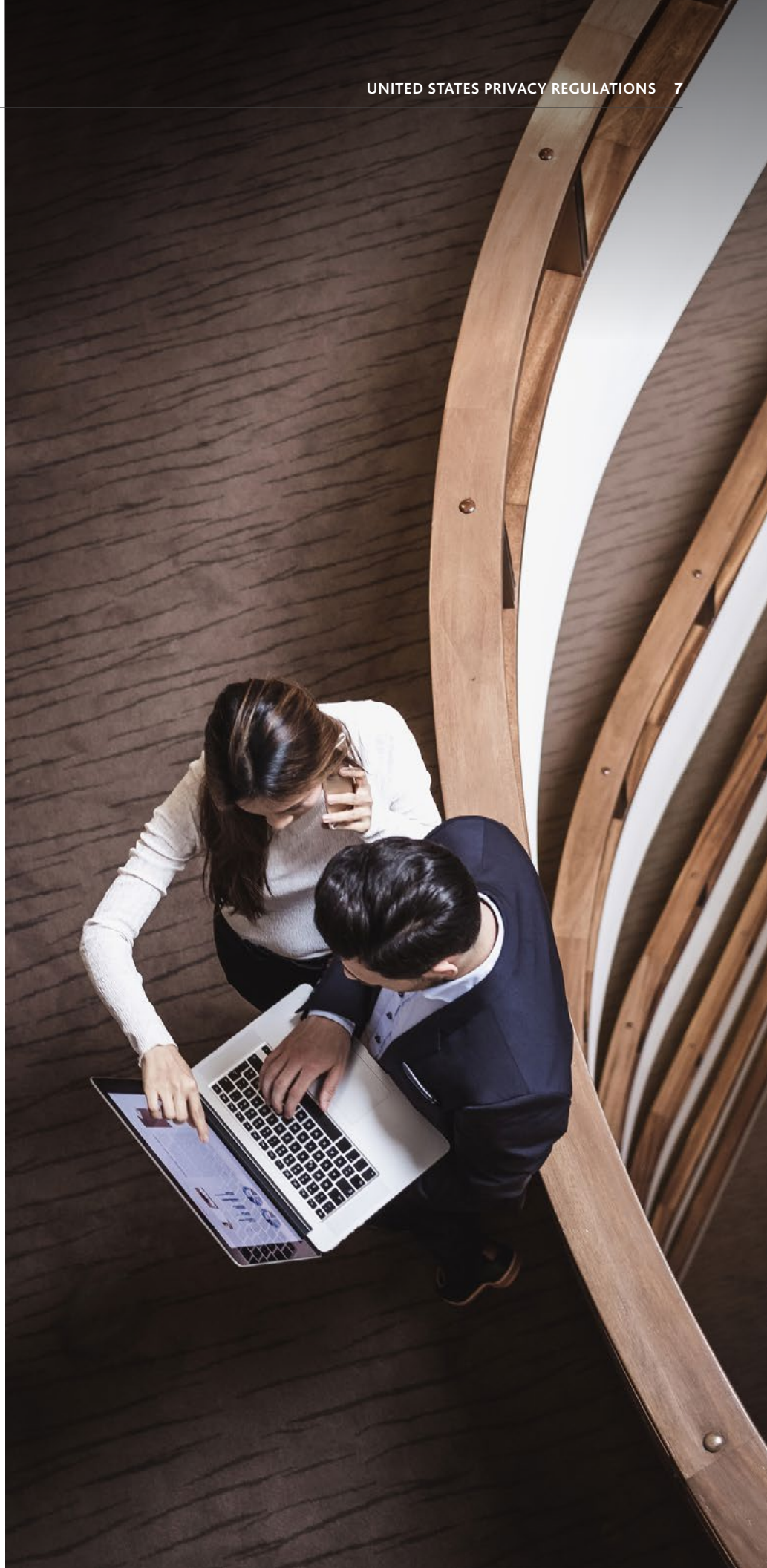
- Don't use false or misleading header information. Your "From," "To," "Reply-To," and routing information – including the originating domain name and email address – must be accurate and identify the person or business who initiated the message.
- Don't use deceptive subject lines. The subject line must accurately reflect the content of the message.
- Identify the message as an ad. Disclose clearly and conspicuously that the message is an advertisement.
- Tell recipients where you are located. The message must include your valid physical postal address. This can be a current street address, a post office box registered with the U.S. Postal Service, or a private mailbox registered with a commercial mail receiving agency established under Postal Service regulations.
- Notify recipients how to opt out of receiving future email. Messages must include a clear and conspicuous explanation of how the recipient can opt out of receiving email. The notice must be crafted in a way that is easy for an ordinary person to recognize, read, and understand. A menu to allow a recipient to opt out of certain types of messages is allowed but must include the option to stop all commercial messages.
- Honor opt-out requests promptly. Any opt-out mechanism offered must be able to process opt-out requests for at least 30 days after the message is sent. Opt-out requests must be honored within 10 business days. Fees can be charged, recipient cannot be required to provide any PII beyond an email address, or the recipient cannot be made to take any step other than sending a reply email or visiting a single page on an Internet website as a condition for honoring an opt-out request. Email addresses cannot be sold or transferred even in the form of a mailing list. The only exception is that email addresses may be transferred to a company that is hired to help comply with the CAN-SPAM Act.
- Monitor what others are doing on your behalf. If another company is hired to handle email marketing, responsibility to comply with the law still rests with the hiring company. Both the company whose product is promoted in the message and the company that sends the message may be held legally responsible.

NATIONAL BIOMETRIC INFORMATION PRIVACY ACT 2020[6]

On August 3rd, 2020, Senators Jeff Markley and Bernie Sanders introduced the National Biometric Information Privacy Act (NBIP) to regulate the collection, retention, disclosure, and destruction of biometric information and for other purposes. The Act defines biometric identifier as:

- Retina or iris scan
- Voiceprint
- Faceprint (including any faceprint derived from a photograph)
- Fingerprints or palm prints and
- Any other uniquely identifying information based on the characteristics of an individual's gait or other immutable characteristics of an individual

The Act prohibits private companies collecting biometric data of individuals from selling, leasing, and using for advertising purposes such information collected. Private companies must obtain consent of individuals before collecting or disclosing their information. Individuals have a private right of action against companies that violate the protections of the Act and private companies are obligated to safeguard the biometric information they collect similar to how other confidential and sensitive information they collect are safeguarded.



6 S.4400 116th Congress (2019-2020)

CONTACTS

KAREN SCHULER
Principal, Governance, Risk & Compliance Leader
BDO Digital
301-354-2581 / kschuler@bdo.com

MARK ANTALIK
Managing Director, Information Governance & Privacy Leader
BDO Digital
617-378-3653 / MAntalik@bdo.com