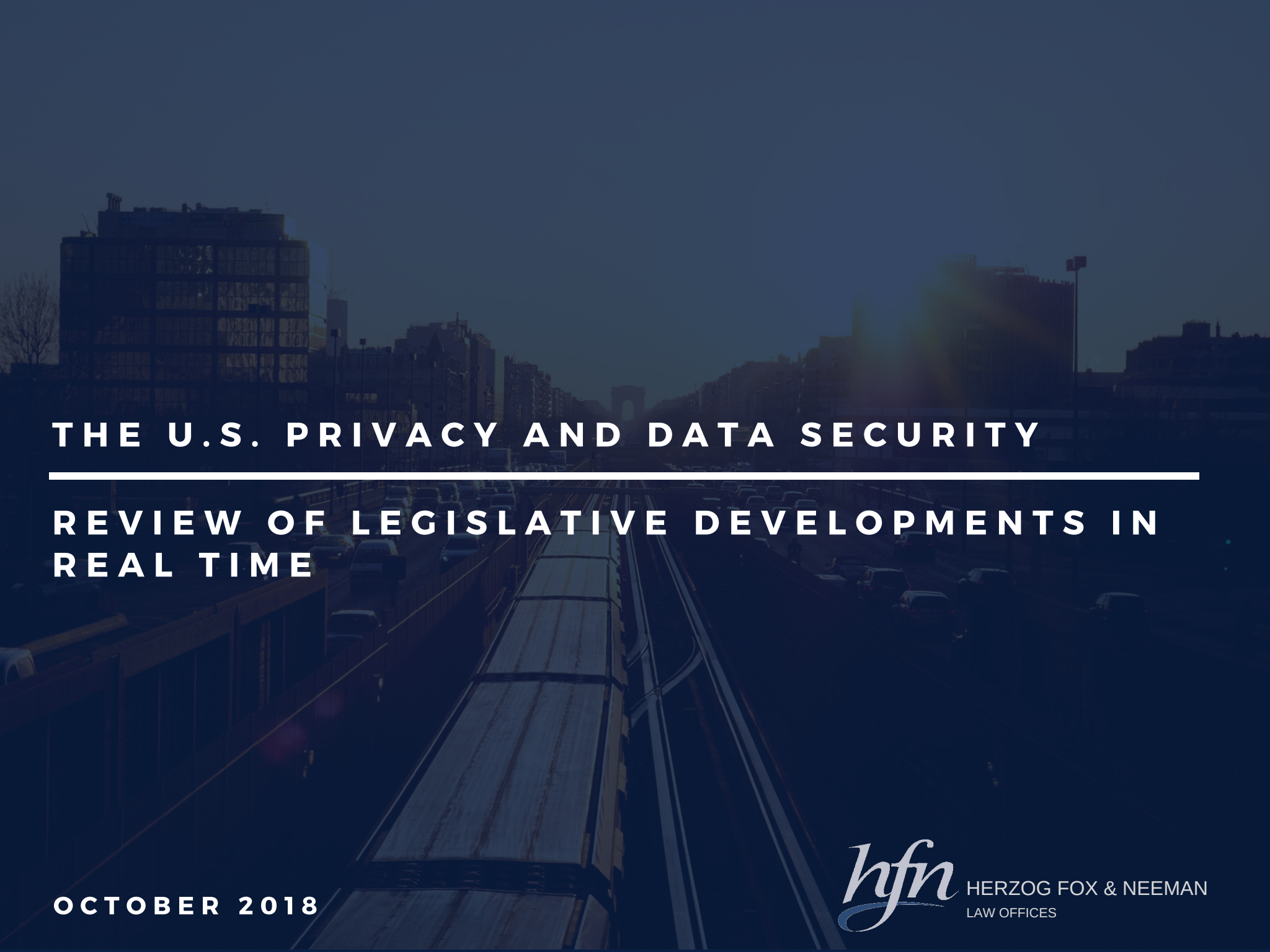

THE U.S. PRIVACY AND DATA SECURITY

REVIEW OF LEGISLATIVE DEVELOPMENTS IN REAL TIME

OCTOBER 2018

HERZOG FOX & NEEMAN
LAW OFFICES

NEW TRENDS IN U.S. PRIVACY LAWS

American legislators and stakeholders have reached the understanding that in today's economic and technological environment, certain gaps in legislation, especially in comparison to the EU legislation (in particular the GPDR) must be bridged. Recent calls (often vociferous) from the public, research institutions, private corporations and elected officials are being heard, and at least in some states, have led to **new data protection and privacy legislation being enacted**.

The new trend has received different interpretations. For example, while **California grants the consumers greater contro**l over their personal data, a different interpretation in **Colorado focuses on entities collecting personal data by applying restrictions** and limitations on them. Another notable regulation is the one which was enacted in **Vermont, the first state in the US that has regulated the market of data brokers**. The latest update in **Ohio's regulation on data protection and privacy sets new and clearer guidelines** for business entities and data collectors. Moreover, the attention of New York's financial sector is currently concentrating on the entering into force of the **New York Financial Services Cyber security Regulation**.

Besides their legal nature and implications, these new regulations also provide helpful guidelines on **how a business should collect and protect personal data**, in specific situations which have not, until now, been regulated in the US. Some of these new regulations also provide some "**safe-harbors**" for businesses operating in the US, or providing services to American consumers.

For companies relying on personal data, **the impact is likely to be significant**. For individuals maybe even more so. However, this new era of data and privacy regulations also gives rise to new and interesting business opportunities, demonstrating that privacy and data protection could become a strategical advantage and help promote and expand one's business and clientele. Within the limited scope of this document, we will try to shed a light on these new legislative trends. During the next months, we will continue to monitor the developments and update this review as this trend continues to unravel.

COLORADO - PROTECTIONS FOR CONSUMER DATA PRIVACY (HB 18-1128)

In effect as of September 2018

Applies To**:** Corporations and individuals processing personal information in the course of their business, vocation, or occupation.

Main Provisions:

1. Expanded definition of personally identifiable information
2. Documentation and retention requirements
3. Security and protection of personal information
4. Enhanced breach notification requirements

OHIO - THE OHIO DATA PROTECTION ACT (S.B. 220)

In effect as of November 2019

Applies To: Businesses that process personal information

Main Provisions:

1. Organizations must implement safeguards, which shall be determined based on the sensitivity of the data retained and the size and complexity of the business
2. Provides an "affirmative defense" from civil liability to entities which implement one of 11 industry-recognized cybersecurity frameworks

NEW YORK – CYBER SECURITY REQUIREMENTS FOR FINANCIAL SERVICES COMPANIES

In effect as of September 2018

Applies To: Entities regulated by the NY Department of Financial Services (banks, insurance companies, investment firms and other financial institutions).

Main Provisions:

1. Enhanced data security requirements
2. Requires maintaining of cybersecurity audit trails and financial records for 3-5 years
3. Minimum regulatory standards for data protection and privacy (such as: security policies and procedures, employee training, access controls, encryption, penetration testing, etc.)

CALIFORNIA - CALIFORNIA CONSUMER PRIVACY ACT OF 2018 (CCPA)

In effect as of January 2020

Applies To: Organizations conducting business in California, that either have an: (a) annual turnover of over $25M, or; (b) handles over 50,000 records of personal information annually, or; (c) derives 50% or more of its annual revenues from selling personal information

Main Provisions:

1. Expanded definition of personal information
2. Provides new data subjects rights:
a. Disclosure of personal data collected
b. Deletion of personal data
c. The right to opt-out
3. New enforcement tools and penalties

NEW YORK – STOP HACKS AND IMPROVE ELECTRONIC DATA SECURITY ACT (SHIELD ACT)

Pending governor's signature

Applies To: Corporations and individuals that hold sensitive personal information of New York residents

Main Provisions:

1. Enhanced data breach notification requirements
2. Organizations must implement "reasonable" safeguards, which shall be determined based on the sensitivity of the data retained and the size and complexity of the business
3. Provides strong incentives to go beyond the minimum, and obtain independent certification that their data security measures meet the highest standards. Companies that do so would get safe harbor from state enforcement action
4. Inadequate security shall be deemed a violation and may give rise to civil action

CALIFORNIA - INFORMATION PRIVACY: CONNECTED DEVICES (S.B. 327)

In effect as of January 2020

Applies To: The first IOT Security Bill in the US, introduces security requirements for connected devices sold in California

Main Provisions:

1. Requires all manufacturers of connected devices to equip their device with reasonable security features appropriate to the nature and function of the device, the information it may collect, contain, or transmit, and to protect the device and any information contained therein.
2. If the device allows remote access, the bill requires it to have unique pre-programmed passwords, or to generate new credentials first login.

VERMONT - AN ACT RELATING TO DATA BROKERS AND CONSUMER PROTECTION (H.764)

In effect as of January 2019

Applies To: Data Brokers, namely businesses that collect, sell or license consumers' data without having direct relationship with them.

Main Provisions:

1. Annual registration
2. Duties to protect personal information
3. Deletion of personal data
4. The right to opt-out
5. New enforcement tools and penalties

HFN HERZOG FOX & NEEMAN LAW OFFICE

HOW CAN YOU PREPARE?

Map and understand your organization's **personal data collection and uses**.

Map your data subjects' **locations and their jurisdiction**. Determine the legislation, regulations and guidelines that apply to you.

Asses the **direct and indirect organizational risks** (for example, likelihood of data breaches from within the organization, and indirect exposure from third party vendors).

Evaluate the existing and update or create new **compliant policies and procedures**. Appoint **data and privacy officers** where applicable.

Redesign **business models and practices** to comply with the regulations.

Leverage the new legislation into new opportunists.

CONTACT OUR TEAM NOW FOR GUIDANCE AND ASSISTANCE ON ANY CYBERSECURITY, DATA PROTECTION AND COMPLIANCE ISSUES!

Asia House, 4 Weizmann St. Tel-Aviv 6423904 | Tel: +972-3-696-6464 | Fax: (972)-3-696-6464
| hfn@hfn.co.il | www.hfn.co.il

ABOUT THE TEAM

HFN's Technology & Regulation team is a recognized market leader in its field. The team is led by domain experts who possess vital regulatory skills and advise startups, multi-national companies, mobile apps and software developers, internet vendors and disruptive technologies, as well as the entire array of the ad supply chain, on various compliance, regulatory and commercial matters concerning technology regulations and compliance, content, app-compliance, e-Commerce, monetization, ad-tech, media and online data protection.

The team has a thorough knowledge and diverse experience of the increasing volume of regulations, enforcement actions and legislative trends in a myriad of jurisdictions, including with respect to heavily "regulated" platforms such as mobile marketplaces, browsers and other platforms, as well as with industry best practices and leading self-regulatory guidelines. This enables the team members to offer unique and practical solutions for often-complex situations and to assist in the development, implementation and management of adequate procedures, thereby mitigating legal and business risks.

OUR TEAM LEADERS

Dr. Nimrod Kozlovski | kozlovskin@hfn.co.il
Nimrod co-heads HFN's Technology & Regulation department and is an expert investor in Cyber Security and a teaching professor on Internet and Cyber Law, Information technology and innovation. Nimrod received his doctor degree in law (J.S.D) from Yale Law School and conducted his Post-Doctorial research in computer science on proactive security at the Yale School of Computer Sciences. Nimrod is also a Partner at JVP, a leading Israeli VC, focusing on Cyber Security and Big Data, and has formerly founded innovative start-ups.

Ariel Yosefi | yosefia@hfn.co.il
Ariel co-heads HFN's Technology & Regulation department and is highly regarded for his global experience in advising multinational companies on diversity of compliance, regulatory and commercial matters concerning technology regulations, including content, app-compliance, e-Commerce, monetization, adtech, media, privacy and online data protection and cybersecurity.

OUR TEAM LEADERS

Ido Manor | manori@hfn.co.il
Ido is a member of the HFN's Technology & Regulation department, and specializes in advising Israeli and international clients, startups and internet companies, on a wide range of regulatory and commercial matters involving data protection and privacy, online advertising, user generated content, social media and mobile marketplaces compliance, e-commerce and international trade.

Israel (Ruly) Ber | beri@hfn.co.il
Ruly joined HFN's Technology & Regulation department after 8 years as a legal advisor in one of Israel's largest banks. Ruly specializes in advising on data protection and privacy, online advertising, user generated content, social media and mobile marketplaces compliance, as well as financial and banking regulations, and their implications on financial institutions' information and technological procedures.

Dan Shalev | shalevd@hfn.co.il
Dan is a member of HFN's Technology & Regulation department, and specializes in advising on various technological and regulatory aspects including online advertising and content, intellectual property, data protection and commercial matters. Dan has started his legal career in working with prestigious Israeli law firms, and has acquired a unique and strategic relevant experience for advising clients in the fields of online media, ad-tech, content and music production, after acting as VP and COO at two well-known ad-tech companies, and after co-founding "Bama" music schools and recording studios.