ACC Association of Corporate Counsel CHICAGO

Data Privacy in the Employment Context

MELISSA SIEBERT
ERIN BOLAN HINES
JEREMY GLENN
KRISTEN HARDER

COZEN O'CONNOR

Today's Presenters

Melissa Siebert
msiebert@cozen.com

Erin Bolan Hines
ebolanhines@cozen.com

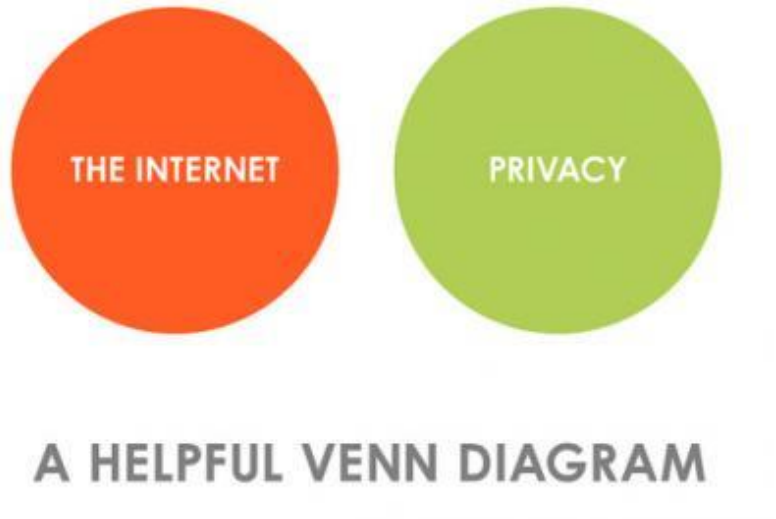
Jeremy Glenn
jglenn@cozen.com

Kristen Harder

COZEN O'CONNOR

Overview of Topics

1. Employee Expectations of Privacy
2. Illinois Right to Privacy in the Workplace Act
3. Illinois Biometric Information Privacy Act
4. BIPA Legislative Reform Efforts



Expectation of Privacy

COZEN O'CONNOR

Employee Monitoring

Common reasons for monitoring employees

- Protect company reputation
- Reduce their exposure to liability
- Uncover potentially disastrous company policy violations
- Pinpoint lost productivity
- Detect declines in employee performance

COZEN O'CONNOR

Employee Data Collection

Common reasons for collecting personal information about employees

- Tax Withholding
- Direct Deposit
- EEO reporting
- Benefit Plan enrollment and claims
- Reasonable Accommodation and medical leave

COZEN O'CONNOR

Employee Surveillance

Statutory Law

- Electronic Communications Privacy Act, (confirms the employer's right to review files and data created by employees during their working hours)
- Illinois Eavesdropping Act, 720 ILCS 5/14 *et seq.* (two-party consent)

Three Types of Common Law – Invasion of Privacy

- Intrusion Upon Seclusion
- Appropriation of Likeness
- Publication of Private Facts

COZEN O'CONNOR

Photo and Video Recording

- **Do employers have the right to use cameras to monitor employee activities?**

  Generally, yes. BUT consider an employee's reasonable expectation of privacy. Some states (Connecticut, California, Rhode Island, West Virginia, Michigan and others) prohibit recording in restrooms, locker rooms and lounges. Also, in a union workplace, likely a mandatory subject of bargaining.

- **Is there a legal difference between hidden and plan view cameras?**

  Yes. The general rule is that an employer may photograph employees in plain view, at their workstations and during working hours, for time and motion studies, or as part of the investigative process. The employer should be able to articulate a legitimate business reason for hidden vs. plain sight cameras.

COZEN O'CONNOR

Photo and Video Recording

- **What can employers use photo and video monitoring for?**

  Generally, to protect against theft, violence and sabotage. But some also use it to track on-the-job performance, internal investigations and for other reasons.

- **What about video *and* audio?**

  Some states (Minnesota and New York) prohibit audio recording of employees without their consent.

COZEN O'CONNOR

WHAT IF?

A Company is concerned about safe operation of its trucks and installs dash cameras that turn on to record video and audio when there is a sudden movement of the vehicle or if the operator turns it on due to hazardous conditions, but the camera inadvertently records her private phone call with a family member about private health and financial matters?

Henyard v. MV Transportation (N.D. Ill. 2019)

COZEN O'CONNOR

Workplace Searches

- **Can an employer randomly search company-owned property without advanced notice?**

  Yes – Generally, employers may conduct workplace searches and interrogations of their employees if there is: (1) a reasonable basis for suspicion of employee wrongdoing, or (2) no reasonable expectation of privacy in the item or thing existed.

- **Can an employer randomly search the employee's property *on company premises* without advanced notice?**

  Generally, no. Employees generally have a reasonable expectation of privacy in their personal items, such as purses, briefcases, and luggage. Therefore, employers generally may not search personal items without a reasonable basis for doing so.

COZEN O'CONNOR

Workplace Searches

Consider the following search of an employee's email folders stored on her work computer:

- The employee had a password protecting access to her work computer
- The employer provided the work computer and allowed limited personal use
- The employer reserved the right to access in accord with applicable laws and legitimate business reasons
- Employee emailed her lawyer about suing the employer.

Sumi Choi v. A University (N.D. Ill. 2020)

COZEN O'CONNOR

What About Electronic Monitoring and Surveillance in the Remote Workplace?

If employers do choose to monitor employees electronically, implement and distribute a clear electronic communications systems policy, pursuant to the Electronic Communications Privacy Act (ECPA), that informs employees that they have no expectation of privacy when using employer-owned resources and provides notice that the employer may:

- review employee emails;
- monitor internet usage;
- track employees' keystrokes; and
- monitor employees' login activity.

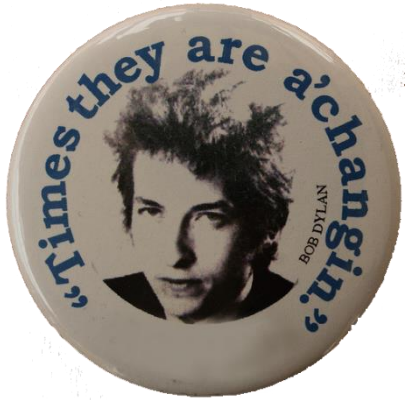
Employers must also ensure that their monitoring of electronic communications and restrictions on employee use of electronic communication systems do not run afoul of employees' rights under the National Labor Relations Act (NLRA).

COZEN O'CONNOR

Best Practices

Employers planning to conduct workplace searches should:

- Advise employees in writing at the time of hire that they should have **no expectation of privacy** in the workplace;
- Outline all areas controlled by the employer that are subject to search (physical such as office, locker, desk, etc. and electronic such as computer, email, phone, etc.);
- Obtain consent (written) from employees for the specific search to be conducted; and
- Have a handbook policy spelling out the consequences for failing to comply with a search request.



COZEN O'CONNOR

A note about Zoom Calls and Privacy

To Record or Not to Record?

Is it eavesdropping? Obtain consent.

At least 12 states require all parties to consent to recording of a conversation: California, Connecticut, Florida, Illinois, Maryland, Massachusetts, Michigan, Montana, Nevada, New Hampshire, Pennsylvania, and Washington.

COZEN O'CONNOR

A Note About Remote Work Monitoring

On October 31, 2022, National Labor Relations Board General Counsel Jennifer Abruzzo announced her intention to protect employees, to the greatest extent possible, from intrusive or abusive electronic monitoring and automated management practices through vigorously enforcing current law and by urging the NLRB to apply settled labor-law principles in a new framework. [*GC Memo 23-02*]

This *proposal* is not the law unless and until the NLRB endorses it. That said, the GC will seek to bring complaints against employers to "tee up" a case for consideration.

Be prepared to explain the business reasons for any electronic management tools – including employees who work remotely or off-site on a regular basis.

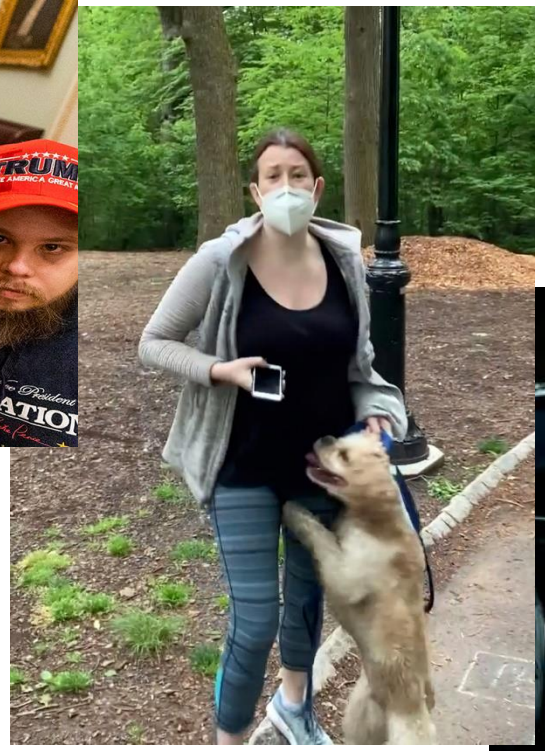
COZEN O'CONNOR

Social Media

"We Used To Live On Farms, Then In Cities, Now We're All Living On The Internet."

COZEN O'CONNOR

When An Employee Goes Viral

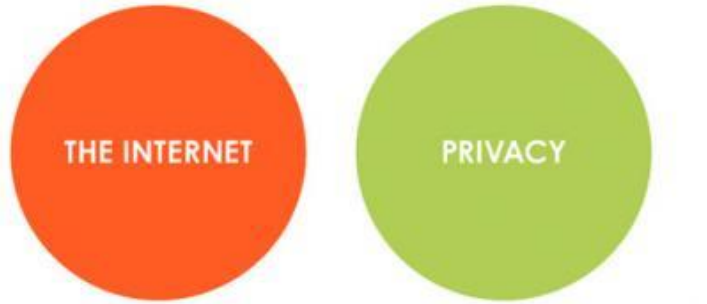


When is employee speech protected?

Title VII of the Civil Rights Act of 1964

First Amendment Freedom of Speech

National Labor Relations Act



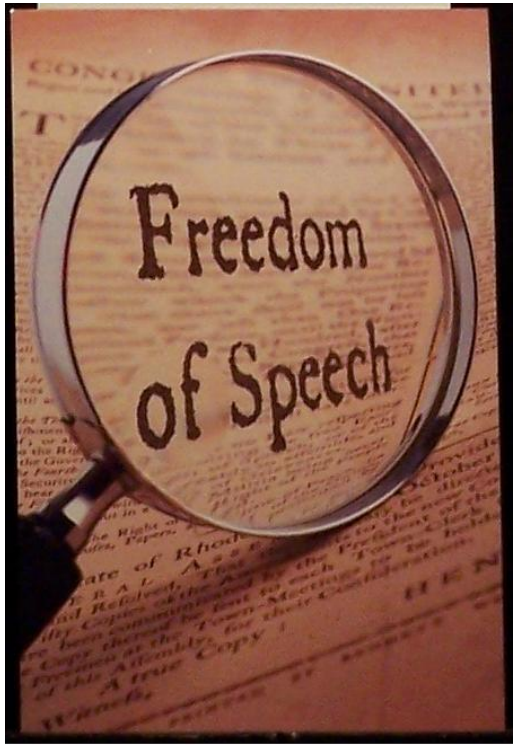
A HELPFUL VENN DIAGRAM

COZEN O'CONNOR

First Amendment Free Speech

Private Employer:

- 1st Amendment **DOES NOT** apply to private employers
- At will employers have latitude to regulate conduct (inside and outside of work) that violates its policies *so long as they are consistently applied*
- Employers have the right to expect their employees perform the duties for which they were hired during work time
- Allowed to prevent the disclosure of confidential information



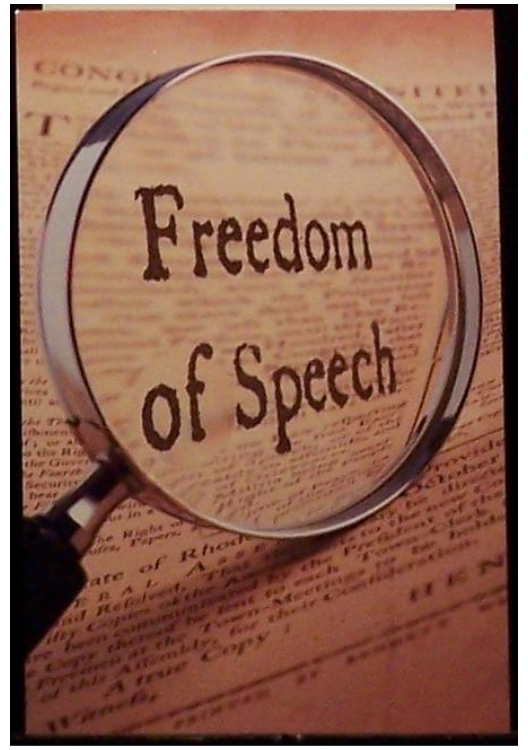
COZEN O'CONNOR

First Amendment Free Speech

Public Employer (federal, state or local government):

- 1st Amendment Freedom of Speech on Matters "of a Public Concern"
- Balance the state employer's interest in a disruption free workplace and the citizen's ability to speak on matters of public importance

- Content of Speech may lose protection of the law (*e.g.* threats of violence, speech that may provoke violence, child pornography, defamatory speech, etc.)



COZEN O'CONNOR

Title VII of the Civil Rights Act

Under Title VII, employers have a **duty** to ensure their work environment is free from discrimination, harassment and intimidation based upon a protected category.

Employers are **required** to take action when necessary to eliminate or redress employee harassment.

COZEN O'CONNOR

National Labor Relations Act

The NLRA applies to almost all employees regardless of whether or not they are unionized (exception: supervisors and independent contractors).

Section 7 of the NLRA grants employees the right to 1) form, join or assist unions and 2) **engage in concerted activity for their mutual aid and protection.**

- Concerted Activity – two or more employees acting together to try to improve their wages, hours or conditions of employment, including:
  - Protesting to improve working conditions
  - Criticizing working conditions
  - Discussing wage rates, bonuses or employment benefits with other employees
  - Complaining about favoritism, specific managers or policies

Applies to both unionized and non-unionized employers

COZEN O'CONNOR

Social Media Discipline - Questions to Ask

- Does the post relate to working conditions or wages?
- Would the post be considered harassment if said face to face?
- What does the policy say?
- Who is the author?
- Do I have a copy of the tweet or post?
- Are we being consistent?

COZEN O'CONNOR

Illinois Right to Privacy in the Workplace Act

- Prohibits employers from discriminating against employees for engaging in **lawful activity outside of work**.
- Prohibits employers from:
  - Acquiring or requiring workers to disclose their **username and passwords** for personal online or social media accounts;
  - Requiring an applicant to **access their personal online or social media account** with the employer present;
  - Requiring an employee or applicant to **invite their employer to join a group related to the employee's or applicant's personal online account**; or
  - Requiring an employee or applicant to join or invite the employer to join any account that would allow the employer access to the employee's or applicant's personal online accounts.
  - Misusing an employee's SSN (e.g. make it public, print SSN on an ID card, require use of SSN to access website, transmit an unsecured SSN over the internet, etc.)

COZEN O'CONNOR

And Now, New E-Verify Rules…

On May 8, 2023, the Illinois legislature passed Senate Bill 1515, which would amend the Illinois Right to Privacy in the Workplace Act (820 ILCS § 55) to mandate a specified process employers would need to follow if they choose to take an adverse employment action against an employee after receiving notice from any Employment Eligibility Verification Systems, including E-Verify, of a discrepancy between an employee's name or social security number.

Unless otherwise required by state or federal law, an employer would not be permitted to voluntarily enroll in the E-Verify program or a similar system.

COZEN O'CONNOR

And Now, New E-Verify Rules…

If notice of a discrepancy between an employee's name or social security number and the SSA's records, and the ER takes any adverse action, ER must provide EE with:

A) the specific document or documents that are deemed to be deficient and the reason why they are deficient;

B) instructions on how the employee can correct the deficient documents;

C) an explanation of the employee's right to have representation present during the verification or re-verification process; and

D) an explanation of any other rights the employee may have with the verification or re-verification process.

Importantly, the employer must also grant the employee no less than 30 days of unpaid leave to correct any verification discrepancy.

COZEN O'CONNOR

The Biometric Information Privacy Act (BIPA)

BIPA & EMPLOYERS

COZEN O'CONNOR

What BIPA Covers

Biometric identifiers – fingerprints, scans of hand/face geometry, iris/retinal scans

Biometric information – Information based on biometric identifiers, regardless of how the information is captured, converted or stored, **used to identify an individual**.

COZEN O'CONNOR

BIPA – The Substantive Requirements

BIPA requires:

- BIPA Section 15(a): Data **possessors** must have a policy re: destruction and retention of biometric data and follow the policy.
- BIPA Section 15(b): Data **collectors/obtainers** must obtain informed consent to data collection, use and storage.
- BIPA Section 15(c): Data **possessors** cannot sell/profit from sale of biometric data.
- BIPA Section 15(d): Data **possessors** need consent prior to disclosure of data.
- BIPA Section 15(e): Data **possessors** must use reasonable care to store, transmit and protect biometric data from disclosure.

COZEN O'CONNOR

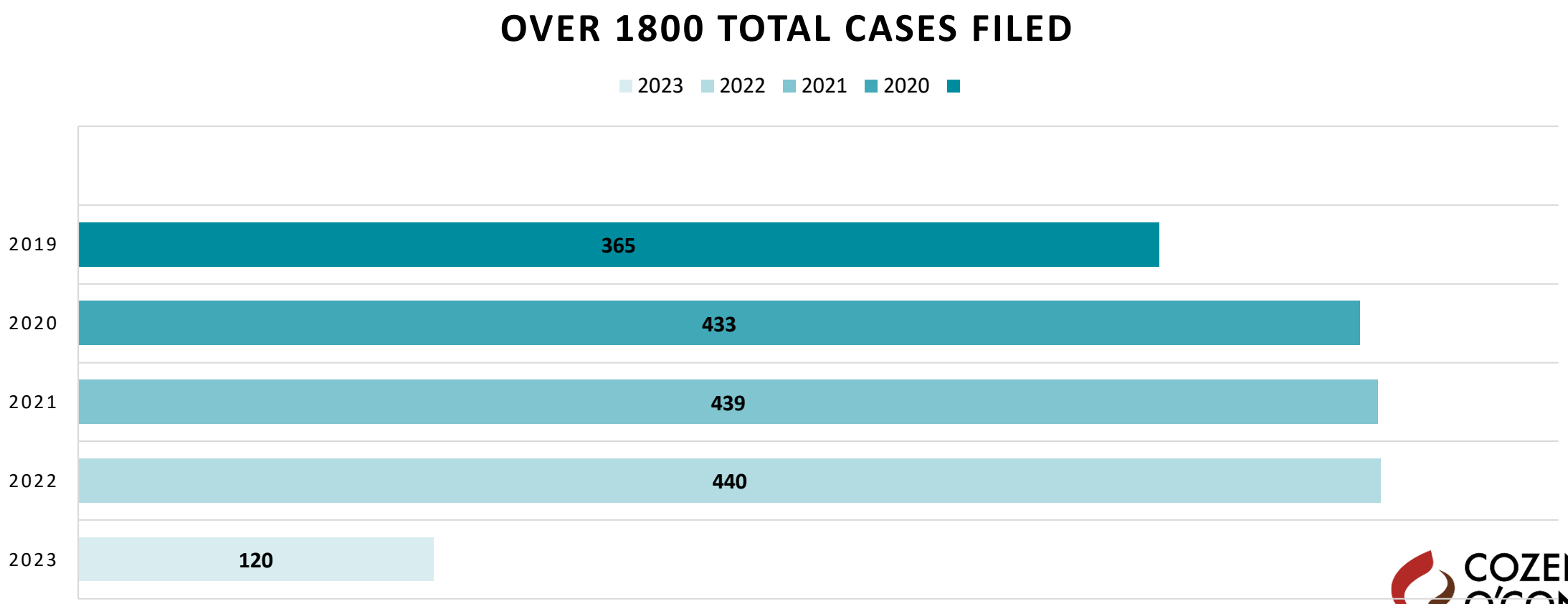
BIPA – Damages

BIPA Section 20:

- Any **aggrieved individual** can bring a class action – no cure period, no data breach required.
- Courts **may** award $1,000 or $5,000 for **each violation**, depending on whether defendant was **negligent or reckless**.
- Prevailing plaintiff entitled to attorneys' fees and expert fees.
- Injunctive relief available (and is routinely requested).

COZEN O'CONNOR

BIPA Lawsuits Filed by Year



BIPA Claims Against Employers

Employers have been sued under BIPA for the following:

- E-signature technology employees use to sign company documents.
- “Biometric” timekeeping systems commonly used to prevent buddy-punching.
- Automated temperature technology during the COVID pandemic.
- Use of facial recognition to access secure areas or company computers.
- Voice recognition systems used in warehouses.

COZEN O’CONNOR

One Employer's BIPA Story

Blommer Chocolate Company

- BIPA compliance
- Lawsuits & attorney demands
- Challenges to electronic signature
- Challenges to policy language
- Best practices/lessons learned

COZEN O'CONNOR

Cothron v. White Castle Explained

What *Cothron* held:

A claim accrues each time that biometric data is collected or disclosed without informed consent.

Damages are discretionary, not mandatory.

The Illinois Legislature needs to clarify how to calculate damages under BIPA.

What *Cothron* **did not hold**:

"Per scan damages" are permitted.

BIPA damages can be calculated in a manner that bankrupts companies.

Courts can only award $1,000 or $5,000 per BIPA violation, nothing less.

COZEN O'CONNOR

BIPA Legislative Reform

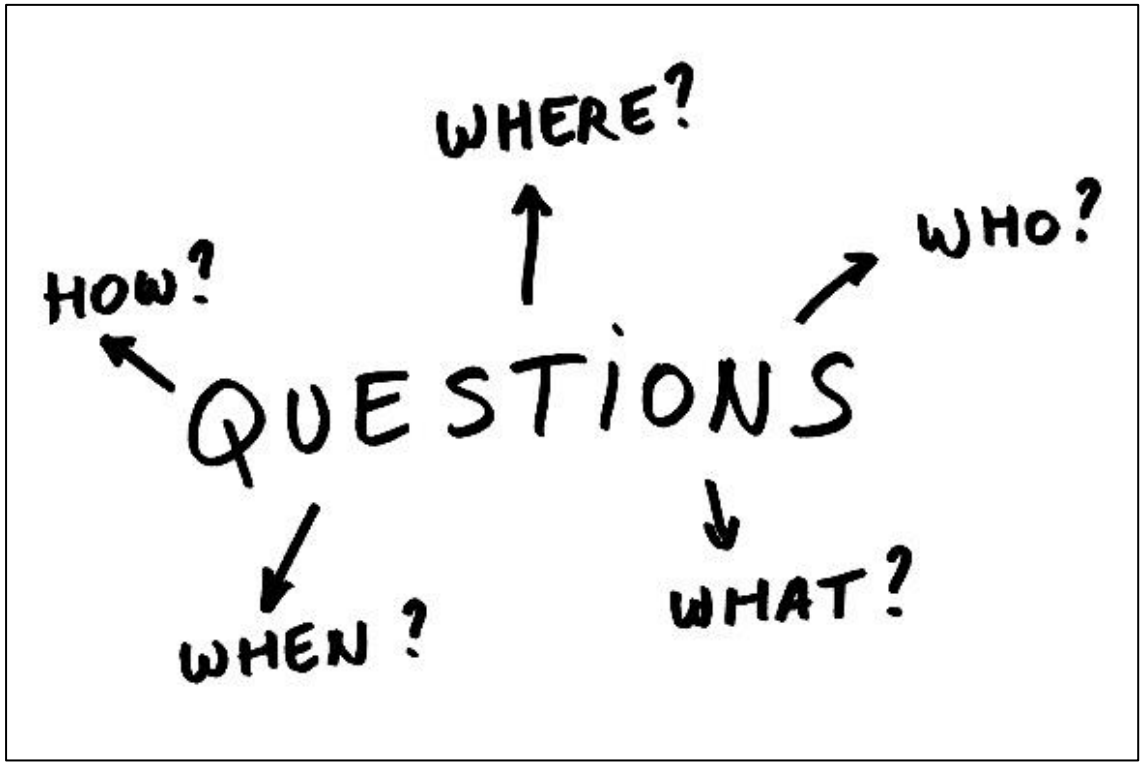
We Got Close!

HB 3811

- Single damages accrual
- Negligence damages increase to $1,500 per section of BIPA
- Electronic signatures presumed valid

Sounds Great! Why It Didn't Pass & What Happens Next.

COZEN O'CONNOR



COZEN O'CONNOR