AMUNDSEN DAVIS

Leadership & Management Certification Training Series

Session 3: Understanding and Implementing AI and New Technology in the Workplace

October 9, 2024

Speakers:

Mike Bendel, Partner, Intellectual Property
John Ochoa, Partner, Cybersecurity & Data Privacy

AMUNDSEN DAVIS

Are Your Employees a Threat to Your Intellectual Property? Is AI?

Michael Bendel

Agenda

Overview of Intellectual Property (IP), Its Value, and PYA

- NDA-CDA / Contract
- Trade Secret
- Copyright
- Trade / Service mark
- Patent

IP Ownership & Scenarios

IP Best Practices Over the Employee Lifecycle

AMUNDSEN DAVIS

What Is IP?

Rights associated with intangible assets owned by a company or a person

Why is IP important to your clients?

- Proactive Company
  - Adds value to the company
  - Mitigates threats from the competition
  - Mitigates internal threats
  - Immediate plan to react if there is an issue
- Reactive Company
  - Risks of infringement
  - Potential decreased value
  - Lack of remedies

The Business Case Is…

Where are you now?

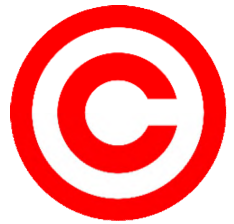
Where do you want to go?

IP helps you get there, or not, by …

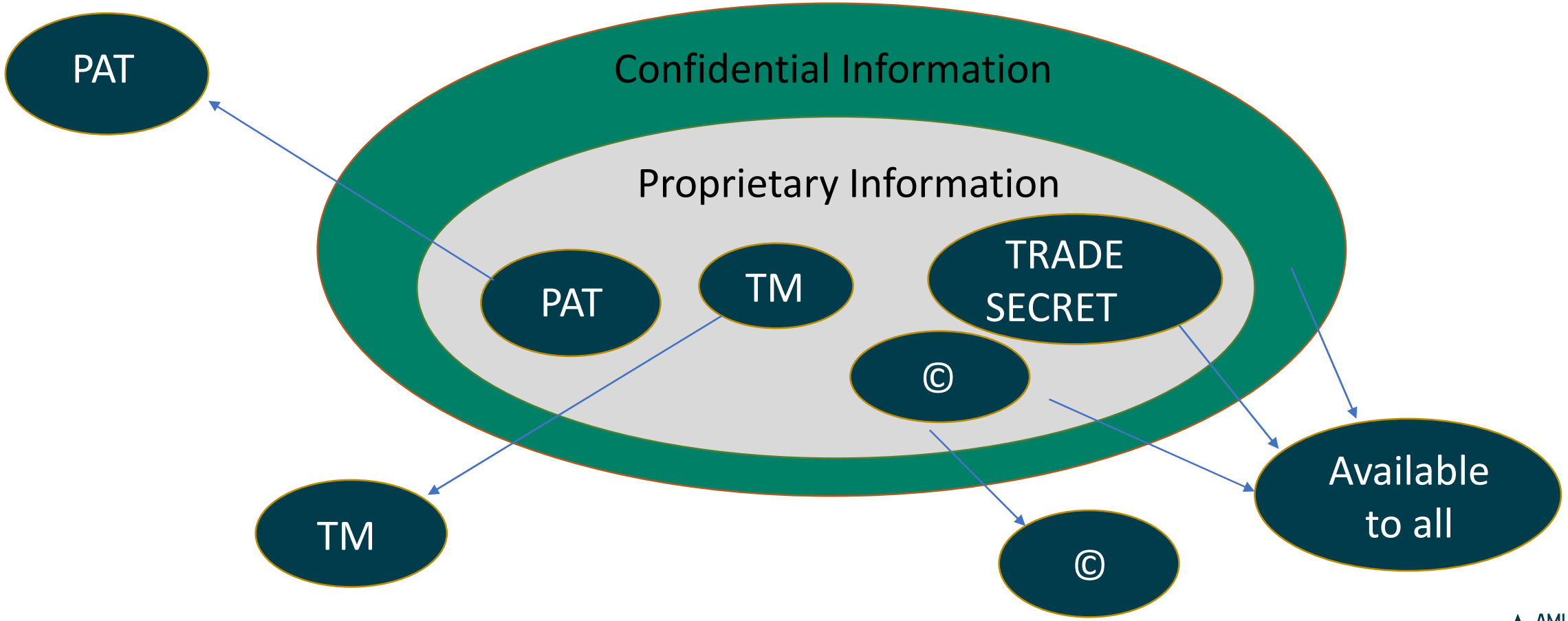
Intellectual Property Is…

- A group of legal rights that provide protection over things people create or invent.

- Key types of IP are:
  - Trademark
  - Service Mark
  - Trade Secret
  - Copyright
  - Patent



The World of Information Is…



NDA/Contract

- **Agreement** between at least two parties prescribing the **use of confidential information** and/or their actions relative to each other and the marketplace.

AMUNDSEN DAVIS

NDA/Contract Value Is…

Very affordable, cost of doing business

Very flexible, two parties agree to…

BUT, only binds contracting parties

Protect Your Assets (PYA) – NDA/Contract

- Use NDA/contract **BEFORE sharing** – employees & contractors!
- Use development agreement **BEFORE collaborating**
- Awareness of existing contracts and terms
- Provide training and reminders
- Exit interview

Trade Secret

Information **not generally known** to the public that gives **economic benefit** to its owner and **reasonable efforts** are made by the owner to maintain its secrecy.

Trade Secret Value Is…

- No registration or fee costs
- Go into effect upon creation, can last forever
- BUT, must take reasonable secrecy measures

AMUNDSEN DAVIS

PYA – Trade Secret

- Trade secret lists
- Internal policies for identifying secrets
- Control access policy and procedures
- Provide training and reminders
- Exit interview

Copyright

- Protects **original works** of authorship **fixed** in a tangible medium of expression for a limited time.

2018 XYZ Co.

All Rights Reserved.

Copyright Value Is…

- Free and automatic upon creation
- If registered, statutory damages
- BUT, narrow and must register to enforce in court

PYA – Copyright

Internal policy for identifying subject matter - offensive tool scenarios

Contract provisions – employees and contractors!

Provide training and reminders

Trademark/Service Mark

Indicia **affixed to goods**, or used to sell or **advertise services**, to **identify the source** of the goods/services.

Trade/Service Mark Value Is…

- Commercial differentiation and price enhancement
- Low cost and can last forever
- BUT, must police other's use

PYA – TM/SM

Protection policy and timing

Trademark / service mark consistency and misuse – your own and others

Monitor and police marketplace - cease and desist letters

Patent

- You teach others to practice your **useful, new, and non-obvious** invention, you get to exclude others from practicing it for a limited time unless you license them to do so. NOT the right to practice another's patent!

Patent Value Is…

Exclusivity to practice your invention and drive business value

Monopoly pricing, license revenue, cross-license tool

BUT, expensive and teaches others

PYA – Patent

Strategy

- Patent policy and guidance docs – **CONFIDENTIALITY pre-disclosure!**
- Patent estate and processes
- Key projects/developments and IP strategy for each
- Budget particulars, preparation process, report outs, timing
- Continuous improvement initiatives for IP estate management, processes, and budget (e.g., balancing IP filings with IP review and culling, others)

AMUNDSEN DAVIS

PYA – Patent

Tactics

- Invention disclosure harvesting and evaluation, rewards, and recognition
- Patent searching, preparation, prosecution, priority filings
- Patent secondary filings, culling/maintenance
- Patent freedom to operate (aka right to practice) processes

When Creating Be Careful To…

Make records – accurate and dated, corroborated

Research **competitive landscape** early – opportunities and risks

Use NDA/contract **BEFORE collaborating** – contractors and employees

When in Market Be Careful to…

File	File applications BEFORE public disclosure
Consider	Consider all forms of IP protection
Monitor	Monitor competitive landscape – their infringements and your improvements

IP Ownership

IP Ownership

Generally, the creator is the owner unless…

- "Work for hire" and "hired to invent"
- Employee scope of hire ….. type of IP matters too
- **Existing** company info versus **new** to company info
- Employer shop right
- I**ndependent contractor** issues, and now…
- There is **AI**…oh my!

Therefore, get it in writing and know who is doing what!

AMUNDSEN DAVIS

Scenario 1

Made Great, a manufacturer of household furniture, employs Alex, a furniture crafter, to develop new products.

In the course of the employment, Alex develops a cutting template for a new table that is a significant improvement over existing table cutting templates. Templates are key to this industry, usually don't leave a "fingerprint," and are generally maintained confidential.

After leaving the employment with Made Great, Alex is induced by Just As Good, a competitor of Made Great, to disclose the Made Great cutting template.

Any concerns here?

Scenario 1 – Result

RESULT: Because Alex was hired by Made Great specifically to develop new furniture products, the template is owned by Made Great. Alex and Just As Good are subject to liability to Made Great.

- What type of IP action seems likely here?
- Could a non-compete agreement prevent Alex from using/disclosing the Made Great template?
- What if Alex used AI to develop the template?

Scenario 2

The facts being as stated in Scenario 1, Alex is hired by Made Great to analyze the furniture products sold by Made Great's competitors.

After leaving the employment with Made Great, Alex is hired to perform a similar task for Just As Good, a competitor of Made Great.

In analyzing the furniture for Just As Good, Alex relies on the general skill and training acquired during the former employment.

Any concerns here?

Scenario 2 - Result

RESULT: Alex and Just As Good are not subject to liability to Made Great.

- What could a non-compete do here?
- What about an NDA?

Scenario 3

Excellent Stuff is a machine manufacturer.

Chris, who is hired by Excellent Stuff as a machine designer, invents a new chemical valuable in Excellent Stuff's business for use in machines, but not related to machine manufacturing.

Chris terminates the employment with Excellent Stuff and begins work for Better Stuff, a competing machine manufacturer, and assists in implementing the new chemical at Better Stuff's factory.

Any concerns here?

Scenario 3 – Result

- RESULT: Because the new chemical was not the product of Chris's assigned duties while employed by Excellent Stuff, in the absence of an agreement to the contrary (written is best, but verbal can be enough), the rights in the chemical are owned by Chris with limited use rights for Excellent Stuff (shop right).
- Chris and Better Stuff are not subject to liability to Excellent Stuff.

Scenario Take-Away Lessons

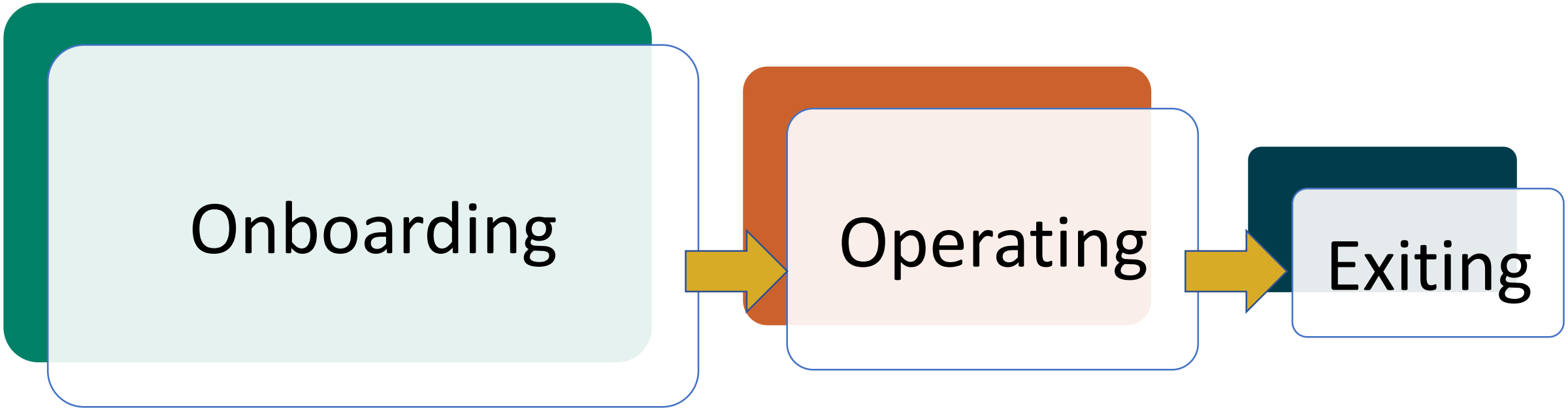
Scenario 1: Hired-to-invent doctrine.

Scenario 2: Employee's right to use general skills and training without liability for trade secret misappropriation.

Scenario 3: Employee's ownership of inventions that were not the product of the employee's assigned duties with the employer's "shop right" to use the inventions if made on employer time or with employer resources.

BOTTOM LINE: Get it in writing! Whatever it is you think you are getting, make sure you know who did what and whether AI was involved.

IP Best Practices Over Employee Lifecycle



Best Practices - Onboarding

Pre-hire/day 1 – Signed confidentiality and IP rights assignment agreement for company IP

Including non-compete/non-solicit obligations for appropriate employees

Train employees on what IP is – specifically, the company IP – and where to find it/how to identify it

Train employees on company IP policies (all employees) and processes (by role)

Personal devices, records to create/keep and where, authorization for spending

Train employees on how to share company IP outside the company

ND obligation, NTK basis, authorization to share out

Best Practices - Operating

Implement a System	• Make identifying IP part of the everyday thinking • Make it easy to use – not a burden
Update Policies	• Stay up-to-date, revise policies as needed • Employee moves within a company may trigger new policies
Know Your Contracts	• Review contracts with third parties to identify IP assets, risks, etc.
Technology	• Keep technology and systems current • Restrict access to IP as necessary and use it to keep trade secrets secret
Education/Know Your Creators	• Tailor training to the right groups • Refresh training with internal employee movement

AMUNDSEN DAVIS

Best Practices – Exiting

- Confidentiality Reminder
- Collection of Confidential Info
- Restriction
- Collect Any Needed Signatures — Inventor/creator? Assignments, Declarations
- Contact Info

IP Best Practices Checklist Discussion

- Reference: Handout 1

AMUNDSEN DAVIS

Closing Questions / Comments ?

- What is unclear?
- What else would you like to know about IP and its interaction with your employees?
- How can we help you utilize your IP better?

AD IP Chart Handout

- Reference: Handout 2

General Information about Key Types of Intellectual Property (IP)

- IP = Intangible assets associated with a company's technological innovation, "brain power" and good will.
- If a company's "intangible assets" meet certain criteria, the law gives the company legal protection.
- 3 attributes: (1) intangible, (2) "right to exclude" and not an affirmative right, (3) personal property.

	TRADE SECRETS	NDA/ CONTRACT	COPYRIGHT	TRADE/ SERVICE MARKS	PATENTS
Gov't	No but...	No but...	Registration (Copyright Office)	Registration (USPTO)	Registration (USPTO)
OVERVIEW	• Great example is Coca-Cola secret formula. • Most technology companies rely on trade secrets as key way to protect IP. • Most fragile form of IP.	• Prescribes use of confidential info and/ or actions of the parties. • Can be most anything they agree to do.	• © is internationally adopted symbol for copyright. • Easier to obtain and cheaper than patent, lasts longer, too. • No infringement if other's work is created independently (without copying).	• Word, name or symbol to identify goods or services. • More expensive and time consuming than copyright, but less than for patents. • Does not protect expression in product (copyright) or underlying invention (patent).	• May obtain a patent on "anything under the sun that is made by man" —U.S. Supreme Court. • Strongest form of IP as defense of independent creation is not allowed. • Most time consuming and expensive IP to obtain, maintain and enforce.
REQUIREMENTS	• Requires reasonable steps taken to protect secrets, such as limited access and NDA. • No registration or filing.	• Mutual agreement and some benefit to each party. • Can be verbal, should be in writing.	• Work not be novel, but must be "original", i.e. not copied. • Creation starts copyright protection, for maximum benefit should use © notice and register work with Copyright Office.	• TM/SM must be distinctive of product/service and not descriptive or generic. • "Fanciful" are strongest marks, followed by "Arbitrary" and then "Suggestive".	• Invention must be: (i) Useful – generally assumed unless it cannot work, (ii) Novel – never been done this way, and (iii) Non-obvious – nothing too close but need not be breakthrough.
PROTECTION	• Federal and state law protects trade secrets through criminal action and civil penalties, against individuals and organizations involved.	• Creates legally enforceable rights just like other IP but only between the parties.	• Protects writing and other forms of expression from unauthorized copying, modification, display and distribution. • Protects the expression of an idea and NOT the idea itself.	• TM/SM my be protected under both state and federal law. • Registration in the USPTO provides the strongest and broadest TM/SM protection.	• Gives owner right to exclude others from practicing the invention (make, use, sell, offer for sale, or import) without license from the owner.
DURATION	• Lasts forever as long as the secret itself is not known to the public.	• Lasts as long as the parties mutually desire.	• For individuals, © lasts life of author + 70 years. • "Works made for hire" © lasts the shorter of 95 years from publication or 120 years from creation. • Jan. 1 1978 is key date.	• TM/SM protection is established as soon as mark is used (common law rights). • Rights last as long as mark is in use and it does not become descriptive or generic.	• Utility patent filed after 6/7/95 lasts 20 years from filing date (else 17 years after grant date). • Design patents filed before 5/13/2015 last 14 years from grant (else 15 years from grant).
CAUTION	• Anything that can be reverse engineered once in public. • Widely known internal "Confidential" info.	• Cannot require illegal activity. • Takes time to reach agreement of parties so plan accordingly.	• Ideas wrapped closely with expression of the ideas. • Just because something is on the web doesn't mean it is free for use.	• Creative works without source identifying purpose/use. • Features that are more functional than source identifying.	• Mere "ideas" without details. • Treating patent types alike, as provisional, design, plant and non-provisional serve unique purposes.

INCREASING PROTECTION AND INCREASING COST

BIPA, GIPA, and Website Accessibility

John Ochoa

How Your Employees and the Feel About Their Privacy

The Illinois Biometric Information Privacy Act

What is the Illinois BIPA?

- Passed in 2008 to protect against risk of identity theft resulting from biometric technology
- Applies to any “private entity” that collects, stores, or uses biometric information as to any individual in Illinois
- Applies regardless of how the biometric information is collected, stored or used and irrespective of the reason for the usage

Pop Quiz:

Which one is NOT biometric information?

A. A person's fingerprint
B. The length of a person's fingers
C. A person's voice
D. A picture of a person's face
E. All the above is biometric information

AMUNDSEN DAVIS

ANSWER:

D – A person’s face

What is Defined as Biometric Information Under BIPA?

- Includes:
  - Retina or iris scan
  - Fingerprint
  - Voiceprint
  - Scan of hand or face geometry
- Does NOT include:
  - Photographs
  - Writing samples

Why Does Illinois Have a Biometric Privacy Act?

- To protect these personal and/or sensitive biometric information
- Because this information is biologically unique—unlike passwords or social security numbers—if they are compromised, it leaves no recourse (i.e., you can't change your fingerprint)

As a Business, What Can and Can't You Do With Biometric Information?

4 primary requirements for businesses when handling biometric information:

1) Informed, signed written consent before collection of biometric information
   - Subject is informed that biometrics will be collected,
   - States the purposes and length of time that biometrics will be kept
   - Written release required by the individual
2) Must have a written policy in place if you possess biometric information
   - Policy retention schedule
   - When the biometrics will be destroyed
3) Cannot disclose or share biometric information without consent
4) Must store biometric information securely

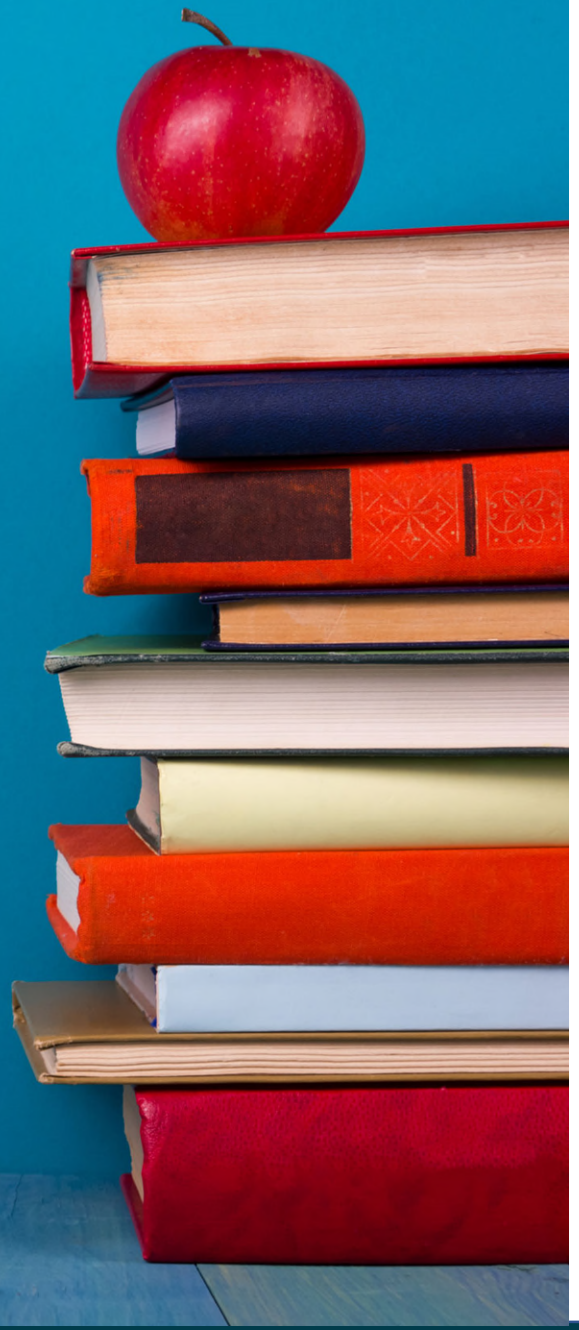
BIPA Reaches Beyond Illinois

- Your physical presence in Illinois is **not** required!
- Questions to ask yourself:
  - Do you collect, capture, purchase, store, possess, or receive biometric data of Illinois residents?
  - Do you have any Illinois employees?
  - Does the transient nature of employees affect you?

Pop Quiz:

From 2008-2014, how many BIPA class actions were filed?

A. 115
B. 32
C. 0
D. 11



AMUNDSEN DAVIS

ANSWER:

C – Zero

Pop Quiz:

How much money has been recovered in BIPA class action lawsuits in the last four and a half years?

A. $0
B. <$50 million
C. <$100 million
D. >$800 million

AMUNDSEN DAVIS

ANSWER:

D - >$800 million

Types of Cases Being Filed

- Timeclock lawsuits (most common)
- Voiceprint lawsuits
- Facial geometry scans and recognition
- As plaintiffs run out of companies to sue, they are branching out to more obscure targets

Why Is This All Happening Now? Driving Forces

- LARGE damages for violations of the statute:
  - $1,000 per violation for negligent violations
  - $5,000 per violation for intentional violations
  - Allows a plaintiff's attorney to recover their attorney's fees if they prevail
- Highly desirable for a class action—odds are if a company is collecting biometric information on one individual, it is collecting it on many individuals

What Have the Courts Said About BIPA?

Illinois courts have issued a series of plaintiff friendly decisions concerning BIPA.

- Courts have held that there is a 5-year statute of limitations on BIPA claims. *Tims v. Black Horse Carriers*.
- Courts have held that a plaintiff does not need to demonstrate they suffered any "actual harm" or damages to state a claim. *Rosenbach v. Six Flags*.
- Courts have suggested that a new violation occurs every time a person scans their fingerprint. *Cothron v. White Castle*.
- These cases rarely go to trial, and almost all are settled prior to trial.

Rinse, Repeat

- Cases are generally settling for between $800-$1,200 per class member, unless there are unique circumstances that push that settlement amount higher or lower.
- Hundreds of millions of dollars, if not over a billion dollars, has collectively been paid out as a result of BIPA lawsuits in Illinois over the past 5 years or so.

Making BIPA History: *Rogers v. BNSF Railway Company*

- The first BIPA case that went to verdict, and lost.
  - The plaintiffs accused the railroad company of collecting driver's fingerprints when they accessed BNSF's facilities. They stared at a judgment of over $200 million.
- One June 2023, the court overturned the $228 million in damages and stated because damages under BIPA were discretionary, "BNSF [was] entitled to have a jury determine the appropriate amount of damages."
- Ultimately, the parties settled, shaving the $228 million exposure down to $75 million.

Recent Amendment to BIPA

- The Illinois legislature recently passed an amendment clarifying that a plaintiff could only recover damages for the *first violation* of the statute.
- There was uncertainty prior if, for example, a person who clocks in and clocks out using their fingerprint could recover damages for *every time* that person clocks in or out. The recent amendment clarifies that one can only recover damages for only the first violation.
- Currently, there is an open question as to whether this will have any retroactive effect.

How Do I Comply with BIPA?

- Before obtaining or using information, provide each person written notice that biometric information will be collected/stored/used, including an explanation of the purpose of its collection and the length of time
- Prior to collection, obtain the individual's express written authorization to collect and store their biometric information

How Do I Comply with BIPA?

- Develop and make **publicly available** a **written** policy establishing a retention schedule and guidelines for destroying biometric information
- Private entities are **prohibited** from disclosing or sharing biometric information with third parties without the **prior consent** of the individual
- Comply *now*! Texas, Washington, California, and many other states have disclosure requirements for the collection, use and storage of biometric information

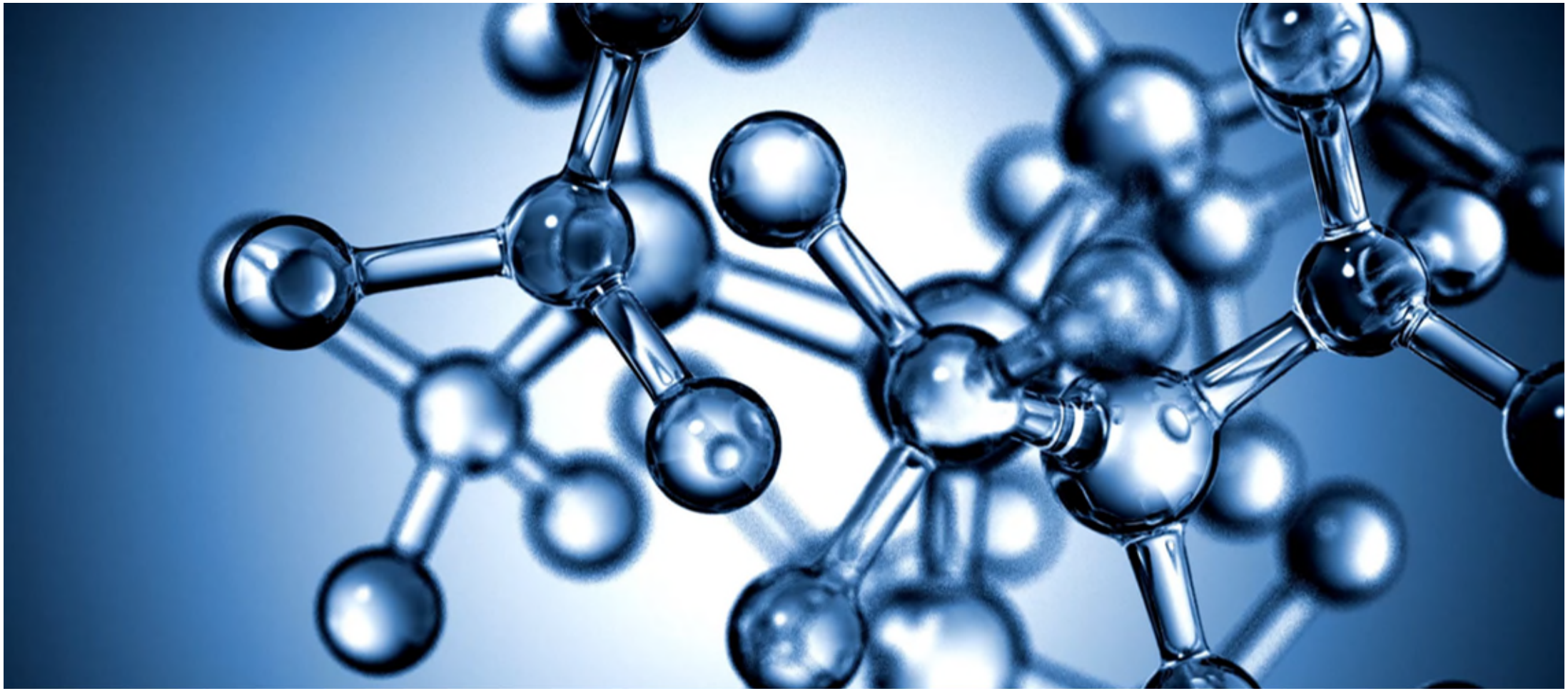
How Do I Comply with BIPA?

- Use the same data security precautions or measures that the company uses for "other confidential and sensitive information"
- This should go without saying: biometric identifiers are considered personal information, so an unauthorized access of the data could be deemed a breach – and trigger notice protocols
- FTC expects biometric data and information to be protected through "privacy by design"

Some takeaways…

- Consider what data you collect and store from consumers, customers and employees and evaluate whether it could be considered biometric data
  - Be overinclusive!
  - Transparency, whether a legal requirement or not, is now the name-of-the-game
- Review your contracts with any third-party vendors that could be relevant to these disclosure requirements

Introduction to the Illinois Genetic Information Privacy Act (GIPA)



Setting the Stage: The Illinois Genetic Information Privacy Act

- There are laws that are appealing to plaintiff's lawyers because they provide for large damages, and could potentially be applicable to a wide range of conduct, which may not be so obvious.
  - BIPA is a prime example—while passed in 2008 and sat dormant for many years, plaintiff's lawyers caught on to employers implementing new biometrics technology for timekeeping purposes. With $1,000-$5,000 per violation, filings in Illinois are still going strong.
- Enter: The Illinois Genetic Information Privacy Act
  - May very well be the next statute used by plaintiff's counsel to grief businesses.
  - Has all the essential ingredients—large statutory damages, as well as definitions and prohibitions that could be interpreted to cover a wide range of information.

What is the Illinois GIPA?

- Passed in 1998 to protect a person's genetic information from disclosure and to prevent anti-discriminatory practices based on an individual's genetic information
- Applies to any employer that collects, discloses, or uses genetic information as to any individual residing in Illinois

Pop Quiz

Which of the following do you think the law would **not** consider "Genetic Information"?

A. A person's genetic test results

B. The fact that a family member has diabetes

C. Prenatal test results for chromosomal abnormalities

D. A person's diagnosis of autism

Answer:

D

An individual's diagnosis of a medical condition would not be considered "genetic information" under the statute.

The Definition of "Genetic Information" is EXTREMELY BROAD

- Includes not only "genetic tests," but also the manifestation of a disease OR disorder in the family members of an individual
- So, what about your mother's father being bald?

What Can or Can't Employers Do With This Information?

1) Employers cannot disclose the genetic information of an individual to ANYONE ELSE without the individual's written consent (this applies to all Illinois businesses, not just employers).

2) You can't require genetic testing, or require collection of genetic information, as condition of employment.

3) You can't change the terms of employment because of genetic testing or genetic information.

What Can or Can't Employers Do With This Information?

4) You can't classify, segregate, or limit employment opportunities or adversely affect the status of employment based on genetic information.

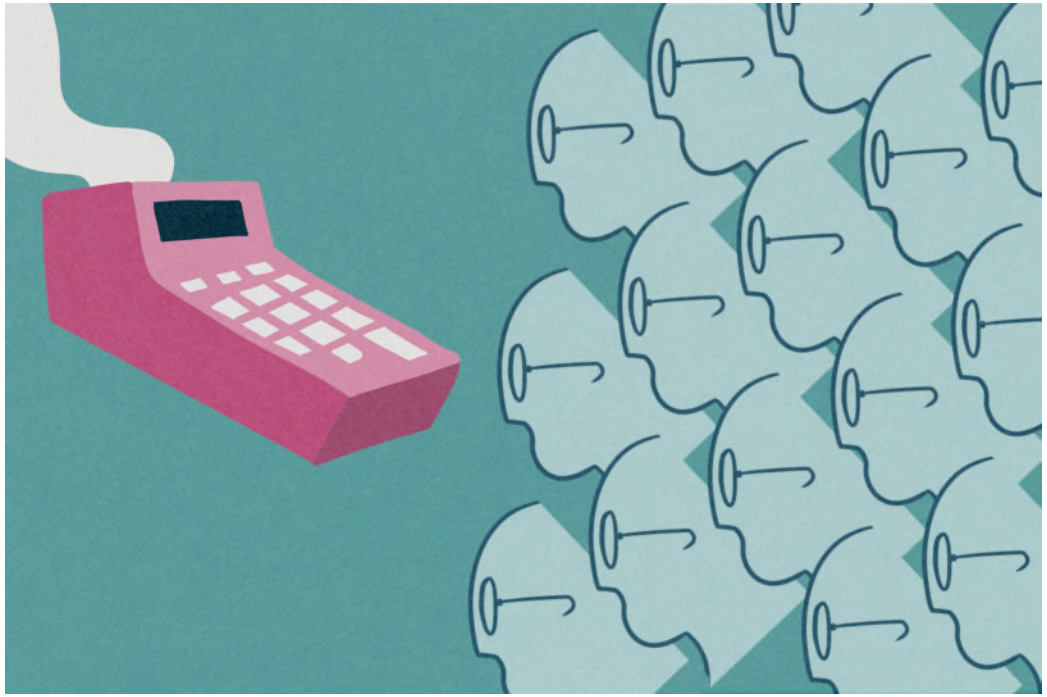
5) You can't retaliate or fire a person alleging a violation of GIPA.

6) You can't offer to pay or benefit in return for taking a genetic test.

Damages Under GIPA

The scary part about GIPA…

- Statutory damages of $2,500 per negligent violation, or actual damages, whichever are greater
- Intentional or reckless violations result in damages of $15,000 per violation
- Prevailing parties can be awarded attorney's fees
- Like BIPA, GIPA has similar per-violation damages structure



Trends in the Law with GIPA Claims

- So far, there have been relatively few claims brought under GIPA compared to BIPA
- HOWEVER, Plaintiffs and Plaintiffs' firms are starting to test this statute

- ***Sekura v. Krishna Schaumburg Tan, Inc.***
  - Notable case because the Court held that a plaintiff need not suffer actual damages to bring a case (much like BIPA).
- ***Bridges et al. v. Blackstone, Inc.***
  - Involved a corporate transaction where Ancestry.com was sold to Blackstone Group. Plaintiff alleged that his genetic information was obtained by Blackstone without his written consent.
  - Court dismissed after finding that Blackstone did nothing wrong by allegedly receiving genetic information.

Trends in the Law with GIPA claims

- In 2023: **Ford, Amazon,** and **Fedex** were all accused of collecting and considering genetic information in the course of the employment application process
  - Plaintiff claims genetic information was collected as condition of employment to decide whether certain employees may be predisposed to certain conditions, such as heart disease, that may make them unable to perform job duties.

Trends in the Law with GIPA claims

- GIPA claims stemming from data breaches
  - Northwestern Hospital lawsuit for an alleged data breach
    - Plaintiffs claimed that, as part of the breach, their genetic information was obtained by third parties. The court denied the defendant's motion to dismiss, and allowed the GIPA claim to continue on the basis that genetic information was likely collected, and compromised, as part of the breach.
  - Settlement involving a GIPA claim that was also a data breach case filed in CA.
    - Illinois residents affected by the breach were entitled to an additional payment of $150 on top of the benefits of being part of the main data breach class (compare that to damages available).

Ultimately, GIPA cases are being brought under several different scenarios, including the job application process, in data breach incidents, corporate transactions, and against companies whose business is to collect and analyze genetic information.

Key Takeaways

What to consider with respect to the Genetic Information Privacy Act?

- Are you collecting your employee's "genetic information"—bearing in mind its broad definition under the statute?
- Do you use wellness programs?
- Do you collect any information in relation to COVID-19 screening?
- Are health screenings offered to your employees?
- Do you collect information for the purposes of determining insurance premiums?
- If so, what are you using it for? Are you sharing the information with anyone else?

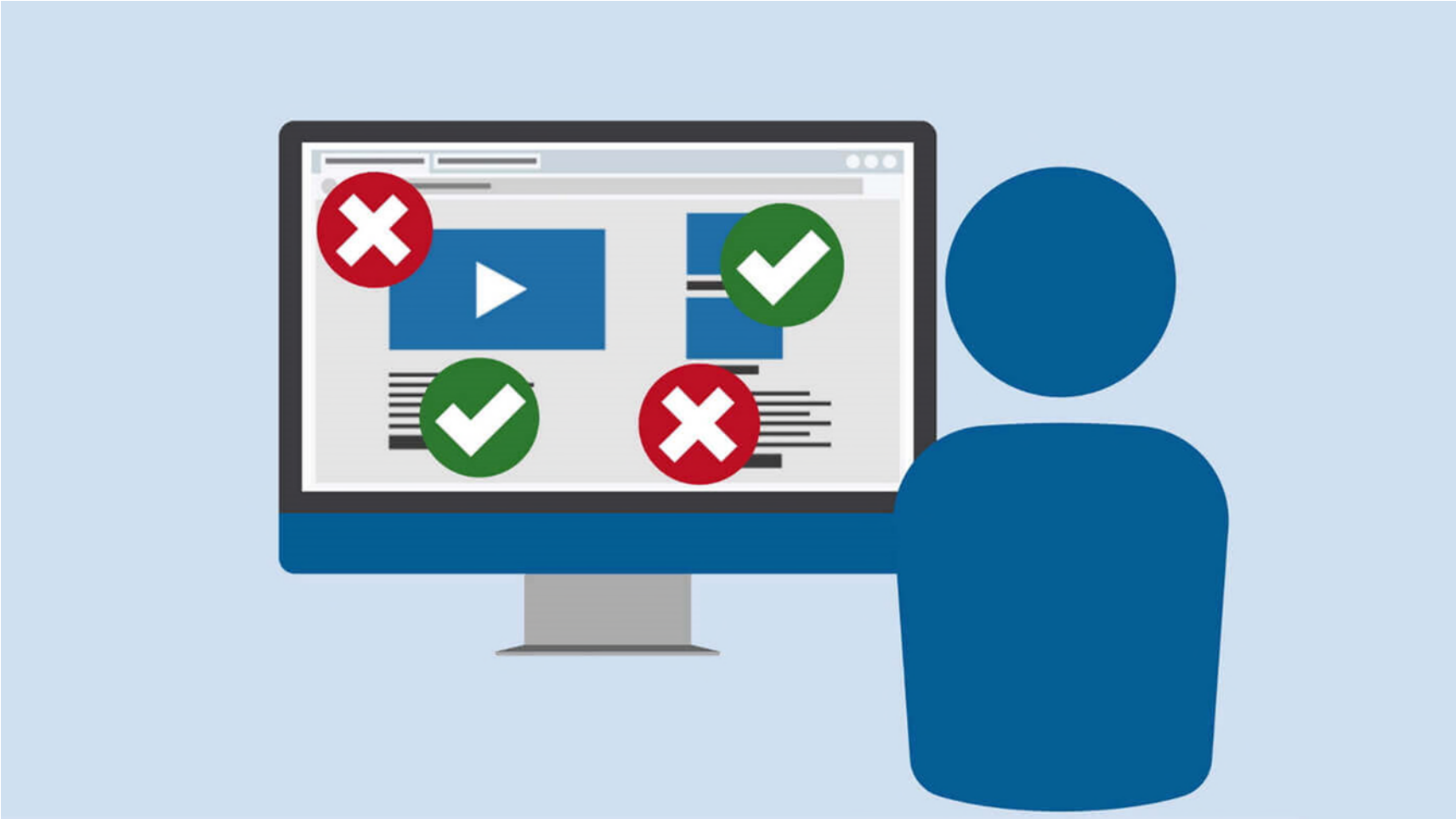
A Word on Wellness Programs and Genetic Monitoring

- You can use genetic information or testing ONLY IF:
  1) You offer health or genetic services
  2) Provide written consent
  3) Information is only disclosed with licensed health care professional
  4) Information cannot be disclosed to employer
- Genetic monitoring is OK, IF:
  1) You obtain written consent
  2) Written notice is provided
  3) Employee is informed of monitoring results
  4) Employer cannot receive any information

Best Practices

- Before collecting, using, or disclosing genetic information, ensure explicit and informed consent from individuals
- Use the same data security precautions or measures that the company uses for “other confidential and sensitive information”
  - Genetic information is also considered personal information!
- Train your organization against discriminatory practices based on genetic information

Website Accessibility Lawsuits



AMUNDSEN DAVIS

Uptick in Website Accessibility Lawsuits

- Increasing number of ADA lawsuits targeting website accessibility.
- Although the ADA was originally meant to apply to "brick and mortar" businesses, the law has evolved to apply the ADA, and other state anti-discrimination laws, to business' websites.

Thus…

If you use a website to interact with customers, that website must be equally accessible to those with disabilities—and most notably, sight-impaired individuals.

The Shakedown…

- Emerging cottage industry appears
  - Sight-impaired individuals and their lawyers are filing thousands of lawsuits per year against website operators of ALL types.

  - Almost identical in nature: Complaint typically alleges that the plaintiff, a sight-impaired individual, was unable to fully access a website and purchase whatever goods or services are offered.
  - Claims are being brought under not only the ADA, but also state anti-discrimination laws, including the Unruh Civil Rights Act in California and the New York State Human Rights Law.

…and the Ramifications

- Laws like the Unruh Civil Rights Act in California and the New York State Human Rights Law provide for damages to plaintiffs, as well as attorneys' fees for plaintiffs' attorneys.
  - For example, expect a minimum $4,000 statutory damages *per occurrence* under the Unruh Civil Rights Act.
- Businesses can expect to pay thousands of dollars to settle these lawsuits, and thousands more to bring their websites into compliance.
- Until websites are made fully compliant, businesses could be subject to "copycat" lawsuits and demand letters from other plaintiffs and plaintiffs' firms.

Best Practices to Minimize Risk and Avoid Lawsuits

1) Collaborate with legal counsel and web development team to make the elements of your website accessible to sight-impaired individuals.

- A good place to start are the guidelines set forth by the Web Content Accessibility Guideline (WCAG).

2) Ensure website contains a statement addressing accessibility and offers sight-impaired individuals alternative means to access your goods and services.

Best Practices to Minimize Risk and Avoid Lawsuits

3) Be aware that web-accessibility overlays (also known as "widgets") may provide a fast solution to making a website accessible, but may not be compatible with "screen readers" and other tools used by sight-impaired individuals to navigate the web.

- This can be a sticky issue in an of itself. In fact, thousands of websites have been sued in spite of accessibility overlays being employed.

4) Perform regular audits of your website to ensure that it remains accessible to sight-impaired individuals.

5) If you do face an accessibility lawsuit, or are sent a demand letter concerning your website, consult with counsel who can assist you in resolving the case and ensuring compliance going forward.

AMUNDSEN DAVIS

Questions?

Thank you for joining us!

Mike Bendel
mbendel@amundsendavislaw.com
920.858.5751

John Ochoa
jochoa@amundsendavislaw.com
312.894.3238