Technology Opportunities/Challenges

- AI & Big Data
- Blockchain
- Cloud Computing (XaaS)
- Mobile Apps
- IoT
- Technology Development & Customization
- Social Media
- e-commerce
- Data Security & Privacy
Scope of Analysis

- **Overarching Question**
  
  What are the *legal barriers* facing electrical product and system manufacturers related to *accessing and using data* generated or collected by their equipment?

- **Areas of Law**
  - Privacy
  - Data Security
  - Intellectual Property
  - Contracts
NEMA Member-Driven Use Cases

1. *Optimization* of product or system performance
2. *Development* of new services or product features for customers
3. *Marketing* existing or new services to customers
4. *Data analytics* for research or commercial uses
Threshold Question

Is the data in question “Personal?”

- Privacy laws **only apply to “personal” data**, defined differently in different laws.

- Over time, the trend is for the definition to become more expansive:
  - Traditional privacy laws cover only “personally identifiable information” (“PII”) – e.g., name, SSN, phone number.
  - More recent laws, e.g. GDPR, CCPA, cover data that is “indirectly” personal – IP addresses, pseudonymized data, etc.
Threshold Question (cont.)

**Is the data in question “Personal?”**

- Many types of data collected by NEMA members are **NOT** “personal” data, therefore not subject to privacy laws.

- This is a fact-intensive inquiry. Examples:
  - Error logs from a factory-line robot
  - Data about the amount of outside air flowing into a building to prevent “sick building syndrome”
  - Smart meter data?
  - If you have to create a personal account or use a personal device to access... e.g. Smart Home apps
U.S. Privacy Law Overview

- Federal and state levels
- Patchwork of laws—no comprehensive federal law
  - Contrast with GDPR in EU
  - It is possible we will see federal legislation soon
- Specifics vary, but the overarching principles are consistent
  - Notice, Choice, Transparency, Access, etc.
Privacy Notices

- One of the universal requirements of privacy laws is that data subjects must be put on *notice* about a company’s data practices.

- Usually this is accomplished through a written privacy policy:
  - Website privacy policies: required under some state laws
  - Can also deliver in-app, onscreen, or in the box

- Direct-to-consumer goods: easy to deliver privacy policies
  - E.g., smart residential thermostat

- What to do where manufacturer has no relationship with data subjects?
Spotlight: California Consumer Privacy Act (CCPA)

- California is in at the forefront of a nationwide expansion of state action on privacy and data security
- Root causes: highly publicized breaches (e.g. Equifax); political scandals (e.g., Cambridge Analytica); global trends (e.g., GDPR)
- CCPA dramatically expands privacy rights for US persons, rivals the EU GDPR
  - Comes into effect in 2020
- Backstory: real estate developer created a privacy ballot initiative, forced legislature to act
- Already amended many times
  - However, radical changes unlikely because they would raise the possibility of another ballot initiative
Spotlight: California Consumer Privacy Act (Cont.)

- Covered data: “information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household”

- Consumers may opt out of “selling” personal data
  - “Selling”: basically any exchange of any of the above data for any consideration
  - Money does not have to change hands

- Other rights: access, deletion, data portability
  - What to do where no direct-to-consumer relationship?

- No class actions for privacy violations, but the California Attorney General keeps any fines (!)
Laws Prohibiting “Unfair or Deceptive” Practices

- State and federal laws prohibit “unfair or deceptive” practices
- At federal level, these laws are overseen by the Federal Trade Commission (FTC), which has interpreted this to give it broad jurisdiction over privacy and data security
- State “mini-FTC acts” mirror FTC but with private rights of action
- “Unfair” practices: Vizio Smart TV tracking
  - Example: always on voice-controlled thermostat
  - Cornerstone: consumer expectations
- “Deceptive” practices: misleading or false privacy policies or statements
  - Gateway Learning case: material changes may not be retroactive
  - Example: smart meter company that said “we don’t use data for marketing” changes its mind
Industry Standards/Codes of Conduct

- For some specific data uses, companies may be contractually or otherwise required to abide by self-regulatory privacy codes of conduct.
- Considering trying to monetize device data by sharing with third-party advertisers?
- What about just using device-generated data for your own marketing efforts?
- In some cases, you may be required to follow the Network Advertising Initiative (NAI) or Digital Advertising Alliance (DAA) codes of conduct, which include additional notice and consent requirements for using data for marketing.
**Surveillance Privacy Laws**

- Electronic Communications Privacy Act (ECPA): prohibits intercepting communications
  - Also governs law enforcement requests for data, which are increasingly common in IoT
- State laws criminalizing surveillance/voyeurism (e.g. NY)
- State tort law: intrusion upon seclusion
Privacy Mitigation Strategies & Best Practices

- Pseudonymization
- Data Minimization
- Privacy by Design
Data Security Law
Data Security Law Overview

- Like privacy law, data security law generally* applies only to companies collecting “personal” data
  - *recent trend may apply data security obligations to IoT companies without any “personal data”
- Federal and state obligations
- States are increasing attention
- Private rights of action
Federal Data Security Enforcement: The FTC

- The FTC applies its “unfair or deceptive” authority to data security cases as well as privacy

- Example (unfair): D-Link “failed to take reasonable steps to protect routers and IP cameras”

- Example (unfair): Lenovo installed **third-party software** on all computers that broke the secure connections between users and websites

- Example (deceptive): Ashley Madison claimed it had “100% secure,” “certified zero risk” private messaging
State Data Security Law: Reasonable Security

- Unreasonable security is actionable under common law negligence
  - What is reasonable?

- Courts often dismiss data security lawsuits for failing to satisfy Constitutional “standing”—plaintiffs not sufficiently injured
  - Example: Ford, GM & Toyota sued for failing to protect vehicle security systems, Dismissed
  - Despite dismissals, the trend is towards allowing such suits to proceed
State Data Security Law: CCPA

- California Consumer Privacy Act (CCPA) allows for data breach class actions
- No federal standing requirement
- Statutory damages $100-750 per consumer per incident!
Spotlight: California IoT Security Law (SB-327)

- Recent development with relevance to NEMA members
- Distinct from California Consumer Privacy Act (CCPA)
- Enacted September 28, 2018
- Like CCPA, comes into effect in 2020
**Spotlight: California IoT Security Law (SB-327)**

- **Who is Covered?**
  - Any “manufacturer of a connected device” (unless covered by HIPAA or other exceptions)
  - “Connected Device” – basically anything connected to the Internet (including indirectly over Bluetooth)

- **What is Required?**
  - Reasonable security that is
    - (1) Appropriate to the nature and function of the device.
    - (2) Appropriate to the information it may collect, contain, or transmit.
    - (3) Designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure.

- Certain password practices are per se reasonable (but not quite a safe harbor)

- Why is this controversial?
Spotlight: California IoT Security Law (SB-327)

- IoT law not limited to Devices with personal data
- Existing California Law already requires reasonable security for personal data
- This intentionally extended data security obligations to non-PI
- Why?
- Takeaways for NEMA
State Data Security Law: Data Breach Notification

- All 50 states, DC and Puerto Rico have requirements to notify consumers and regulators in the case of a data breach

- Two main inquiries:
  - 1. Was the incident a “breach”?
  - 2. Was the data at issue “personal information”?

- “personal information” in these laws is usually limited to traditional “personally identifiable information” categories

- Incident response is costly and can be mitigated by proper planning
Data Security Mitigation Strategies & Best Practices

- Policies & Procedures
- Risk Assessments
- Tabletop Exercises
Threshold Question

Can IoT or machine-generated data be owned?

- What does ownership require?
- Ownership is a **legal concept** that requires a legal framework to exist
  - Hinges on the *existence of a recognizable property right*
- Property law evolved from judicial decisions regarding land and personal property ownership
  - Essentially, decisions about *tangible property*
- But what about *intangible property*?
Tangible v. Intangible Property

- Applying tangible property law concepts to intangible property is largely impossible
  - Why? Example: Can you copy land?
- **Intellectual property law** is the legal framework for owning *intangible property* in the U.S.
- No inherent ownership in intangible property *until and unless*:
  - the data becomes eligible for protection under a recognized *intellectual property right*; or
  - a specific ownership right is allocated by *statute*
- Tort law (civil “wrongs”) illustrates how tangible and intangible property are treated differently
Traditional Property Law Does Not Apply

- **Bots Overworking Computers** – Verio used automated search bots to access Register.com’s domain name database. Register’s property tort claim was **successful** on the theory that the bots would overtax Register’s servers and computing systems – its *tangible property*

- **Scraping Data** – Tickets.com used webcrawlers and spiders used to scrape event information from Ticketmaster’s website. Ticketmaster was **unsuccessful** in its property tort claim because it did not show that the crawlers would harm its physical computer equipment or business

- **Copying an Older Sound Recording** – iHeartMedia duplicated a pre-1972 sound recording (i.e., prior to federal copyright protection for sound recordings). Music artist’s property tort claim was **unsuccessful** because the digital sound recording is “insufficiently tangible property” for a property tort claim to survive
Statutory Ownership Rights

- IP law is based in statute, and has default rules about ownership
- **Rules can always be changed by legislatures**
  - Example: The federal Driver Privacy Act of 2015, included as a small part of the Fixing America’s Surface Transportation (FAST) Act, applies to any data retained by an event data recorder (EDR) (e.g., a black box) installed in a vehicle
- Data retained by the EDR is the “property of the owner” or lessee of the vehicle in which the EDR is installed
- No one else can access the data unless an exception is met (including owner consent)
- Industry-specific laws will underscore importance of *contracts* (as the vehicle for obtaining consent)
IP Overview

In the U.S., there are four types of intellectual property rights:

- **Copyright**
  - Original works of authorship (e.g., books, musical compositions, art)

- **Patent**
  - New, useful and non-obvious inventions, processes, machines, etc.

- **Trade Secret**
  - “Secret sauce” – information that has value because it is not known to competitors

- **Trademark**
  - Words and symbols that identify origin
Copyright in Data?

- Copyright protection of data will turn on these questions:
  - Is the data raw data that reflects only a fact (e.g., device X used 6 gallons of water)?
  - Has the data been compiled into a database?
  - Has the data been further manipulated, processed or refined to create derived data?

- No copyright protection for facts
  - Hallmark of copyright protection is originality, not effort
Copyright: Remember Ticketmaster?

- In the Ticketmaster case, Tickets.com scraped facts about upcoming events from the Ticketmaster website.
- Even though Ticketmaster gathered the data, the event information was just factual – not original works that could be copyrighted.
- Quote: “[r]aw facts may be copied at will”
- Discuss: How could Ticketmaster have protected itself?
Copyright: Data Compilations

- Compiling data does not avoid copyright’s cornerstone: originality still required!

- Databases can be copyrighted, but the database must have some originality in how it is coordinated, selected and arranged
  - Even then, the method of organizing the data is what is copyrighted; the raw data itself is still “free for the taking”

- What kinds of compilations have been copyrighted?
  - Directory of Chinese-American businesses
  - Baseball pitching form with nine columns of various stats
  - Compilation of expected wholesale prices of collectible coins

- But not the white pages, a comprehensive dental procedure taxonomy, or a comprehensive cable system fact book
Copyright: Derived Data

- Derived data has been processed, modified, enhanced, translated – some other derivation of original data
- **If the resulting work is original enough, could be copyrightable**
- Example: Analyses, reports, white papers drawing conclusions from raw data would probably be copyrightable
- Facts and statistics cited in the derived work would still not be copyrightable, but the arrangement and how they are expressed could be
Trade Secrets

- Distinction from copyright: copyright protects original expression of ideas; trade secrets are the very ideas themselves

- What is a trade secret? Two-part definition:
  - Information that has **independent economic value due to being a secret** (i.e., not known to competitors or the industry generally)
  - Reasonable efforts are used to **maintain its secrecy**

- What are “reasonable efforts”?
  - Physical and technical security measures and written confidentiality agreements with anyone who will have access are usually enough
Trade Secrets: Protecting Non-Copyrightable Data

- The most famous trade secret of all is not copyrightable. What is it?
  - Hint: recipes (a “mere listing” of ingredients and quantities) are not copyrightable

- Data sets of device data probably can meet the requirements of a trade secret
  - Does the data have independent economic value because it’s confidential?
  - Does the company use reasonable efforts to keep it secret?

- Trade secrets can also protect the tools and algorithms used to digest big data
  - Even if everyone had the same access to data, only those with the right tools could do anything with it
Trade Secrets: Who Owns Them?

- Assuming there is a trade secret in IoT data, who owns it?
- Likely the company that takes the steps to gather and analyze the data and works to keep it secret
  - Expect this would often be the device manufacturer
- What if you hire a company to analyze your data?
  - Trade secret follows a “hired to invent” doctrine, so the hiring company will own the resulting work
  - But, you should *always specify ownership rights and limitations in the contract* with the partner
Trade Secrets: Limitations of Protection

- Trade secret rights only protect against actual misappropriation (e.g., improper disclosure by a former employee, theft of documents, a breach of a valid confidentiality agreement)
- Does not protect against legitimate reverse engineering or independent development (e.g., gathering or generating the same data in a different way)
- Important to consider expected use – is your company really going to keep the data secret?
- Consider aggregation – if 10 companies aggregate their data sets, exerting trade secret ownership over individual contributions could be difficult
  - A contract would still be required to have confidentiality provisions and clearly define how the companies could use the shared data, and allocating ownership and rights in derived data
IP Mitigation Strategy

- Is IP protection of IoT or device data the answer?
  - Probably not, or if it is, it’s only half the answer
- Contracts are the better choice for defining ownership and use rights in data
  - And even if IP protection is claimed, contracts will still be needed
Contract Overview

- Contract is an agreement between two or more parties
- Very few limitations on what you can agree to do in a contract
- Contracts afford great flexibility and are better than the IP framework for defining ownership and use rights in data
- Protecting data that is not copyrightable or a trade secret? Use a contract
  - *ProCD* case – Michael bought a CD with name and telephone listings from 3,000 directories. CD had a shrink-wrap license around it saying that the user could not further redistribute the telephone listings. Michael made the listings freely available on his own website.
  - Was a copyright claim the answer here? No. Breach of the shrink-wrap license by Michael
Chain of Contracts

- Chain of contracts is required – think about everyone that touches or contributes to the data
  - Manufacturer
  - Resellers and distributors
  - Device purchasers, consumers, end users
  - Data aggregation or analytics partners
- Not just a company-level analysis – every product or service’s contract chain will likely be unique
- Rise in data strategy – template contract development is a vital part of developing a holistic data strategy for your company
End User Terms or Terms of Service

- Terms of sale, use, or service are typically the first link the contract chain
- Contract between manufacturer and the consumer or end-purchaser of the device
- Report outlines several examples from the connected car industry
- Not just important for data ownership – also data-related disclaimers
  - Example: disclaimers of responsibility as to the quality of services based on user data
Machine-Generated Data v. User-Generated Content

- Manufacturer should assert ownership over *device-generated or collected* data in the ToS
  - Manufacturer can clarify that machine-generated data will only be used consistent with the manufacturer’s privacy policy
  - Reinforces need to have a privacy policy that adequately addresses intended uses

- Manufacturers, application developers, social media platforms, and interactive websites generally do not assert ownership over *user-generated or user-provided* content
  - User content is often copyrightable as an original expression (e.g., photo, post, tweet)
  - Social media sites generally say that the user owns her content, but...
  - terms of service also include broad licenses back to the site in order to protect the company’s latitude to use, commercialize, analyze and otherwise exploit user data
Ownership Isn’t Everything

- Does your company actually need to own its device-generated data?
- No – a broad license can also work
- Connected car industry has largely not claimed ownership of device-generated data
  - Instead, user grants a broad license to the company permitting the company to use all user data
  - Wide latitude to create and use aggregated anonymized user data in any manner is often reserved
  - Company limited only by its privacy policy
Data Licenses with Partners

- Data license agreements – frequent vehicles for marketing, aggregation, analytics and commercialization purposes
- Scope of rights granted to data license partners varies widely
- Data license agreements should address **exclusivity**, **sublicensing**, **aggregation** and **modification**, the **creation of derivative data** or derivative works, **geographic or territorial restrictions**, limitations on **number of users or devices**, and the **purposes** for which the licensee may use the data
- Careful review of existing and new agreements is needed because data licenses are often heavily negotiated.
  - A good template is not enough
  - Example: some companies might limit data rights to “noncommercial use,” or usage “necessary to deliver the Services”
Other Contracts and Clauses

- **Confidentiality Agreements**
  - Definition of “Confidential Information” can be overly broad and include things like “all information relating to Customer’s use of the Product”
  - Could then require the manufacturer to keep data generated from the customer’s use of the product strictly confidential

- **Data Processing Agreements**
  - Typically used to meet foreign requirements (like the GDPR)
  - Can be overbroad, and some companies indiscriminately sign or make partners sign them even where GDPR is not implicated

- **Flow-Through Terms**
  - Used to satisfy obligations to people who are not parties to the contract (e.g., employees of the company that purchases a product that will be collecting information from those employees)
Contract Mitigation Strategy

- Identify all of the contracts in the chain
- Review them very carefully
- Harmonize where there are gaps
- Implement a pro-active data strategy at the organizational level
  - Develop a plan to address new contracts, products and relationships
  - Seek out opportunities to amend old contracts to close the gaps
- Have a policy in place with preferred and alternative data ownership and license language
  - Educate procurement, sales, legal, product development, etc. on the policy
Conclusion
Conclusion

- Topic that will be top of mind for IoT product manufacturers around the world
- More and more companies are investing significant time and energy in developing global data strategies
- Data strategy should use a multi-disciplinary perspective
  - Legal barriers and mitigation strategies discussed today should be included in data strategy development
Disclaimer

- This presentation and the associated report *do not establish an attorney-client relationship between McDermott Will & Emery & any NEMA member.*

- This presentation will not preclude McDermott Will & Emery (or any of its legal entities) from representing any other person or company in any matter.

- It will not obligate McDermott Will & Emery to keep confidential any information provided in connection with this presentation.

- This presentation is for *general information purposes only* and should not be construed as legal advice, legal opinion or any other advice on any specific facts or circumstances.
Thank you.