Future-Proofing Pennsylvania

Prof. Andrea M. Matwyshyn

Professor of Law and Engineering Policy, Dickinson Law
Professor, SEDI, Engineering
Founding Director, Policy Innovation Lab of Tomorrow (PILOT)
Penn State
andreamm@psu.edu
andreamm.com

I. "Why are The Normies suddenly so angry about data centers?"

- It's not sudden - simmering since at least 2024.
- Part of a larger Techsploit Triangle with three meanings of "exploit" – computer security, humans, and land/resources

II. Context: Eight warning signs of the Techsploit Triangle are visible in data center buildouts. The litigation is just beginning, and it is well underway in other states. Harms are already happening.

- 1. Underpants Gnomes Business Models; 2. Mystery Meat Products; 3. Panic Building at Socially Destructive Scale; 4. Fruitcake Financing; 5. Unaligned Goals and Body Snatching; 6. Anti-Public Takings; 7. Forgetting Engineering Disaster History; 8. No Shepherd's Pie Planning

III. Three Key Futureproofing Takeaways:

- *Planning*: Look to the (multiple possible versions of the) future and defend traditional safety baselines. Avoid promotion of tech hype/fads: we are likely over-building for a specific, last generation AI model, not for the future. Build around Pennsylvanians' (self-defined) needs, not tech maximization. Pennsylvania is not a Silicon Valley sacrifice zone of "NPCs."
- *Defending democratic process*: Good start - Executive Order limiting NDAs + transparency map.
    - State level: Clarify PA zoning law to enhance local control and scale-based veto rights under "fair share" analysis in non-housing uses, especially if the proposed use potentially harms existing housing and habitability. Destruction of community quiet enjoyment when disconnected from local needs is not offset by tax revenue. End tax incentives for equipment for businesses with 20+ employees and add a "straw purchaser" provision that prohibits resale/ licensing for 3 years.
    - Local level: Expect that this AI bubble is going to pop. The pace is hype/artificial, and what comes next will have different hardware needs. Expect almost complete automation of data centers. Plan for reuse of abandoned projects. Expect high volumes of litigation if data centers are forced onto residents. Beware of cost recovery delays, mass torts, and legal gaming, e.g. Texas Two Step bankruptcy. Consider aggressive surety bond use.

- *Protecting safety*: Data center anger is just a symptom of a bigger problem. Address the bigger tech safety problem in a scalable way: create a new state-level Pennsylvania Bureau of Technology Safety ("PA BoTS"). PA BoTS would focus on tech safety, bottom-up tech competition enhancement, and tech fraud.
    - A different "friendly expert" agency model that is bottom-up and based on technology reality: peer collaboration and gap filling across government - a technology safety regulator of last resort;
    - Nimble, financially self-sustaining, entrepreneurial, and First Amendment sensitive by design;
    - A technology neutral approach that will scale alongside future tech.
    - Corrects unfair under-regulation of big tech compared to traditional industries. Compare (the necessary extent of) food safety regulation – tech has the same issues re: supply chain control, fragility, risk of physical harm. PA has multiple agencies that consider food safety (plus AG), but zero for tech.
    - Addresses rampant technology fraud that is hurting market mechanisms and honest businesses. PA BoTS would facilitate market recognition of safety-first tech companies.
    - PA BoTS would have three branches:
        - Pilot Projects: A community ombudsman to scale information sharing + a (small) team to "future proof" the PA tech economy with bottom-up community led projects solving real problems; "Build the Future" contests and other bottom-up efforts; a Pennsylvania-first, safety-first tech incubator; computer security infrastructure tiger teams to help updating and incident response.
        - Policy Planning and Rulemaking: Rulemaking focused on empowering market mechanisms, e.g. creating uniform public disclosures of baselines of safety and market information integrity; requiring security threat modeling and planning for data center deprecation and reuse. PA BoTS would nudge shared goals with expertise, mitigating tech staff shortages in agencies.
        - Enforcement: Tech safety enforcement to assist/collaborate with/supplement other agencies' work as needed with additional tech expertise, filling tech safety gaps; fraud and deception enforcement in connection with PA BoTS's disclosure-based filings – PA BoTS should have civil and criminal fining authority; tech safety whistleblower office.
    - Two immediate priority areas: (1) data center public nuisance monitoring and mitigation and (2) computer security threat mitigation.
    - Offer: I will "loan" myself out from Penn State to help Pennsylvania launch PA BoTS.