

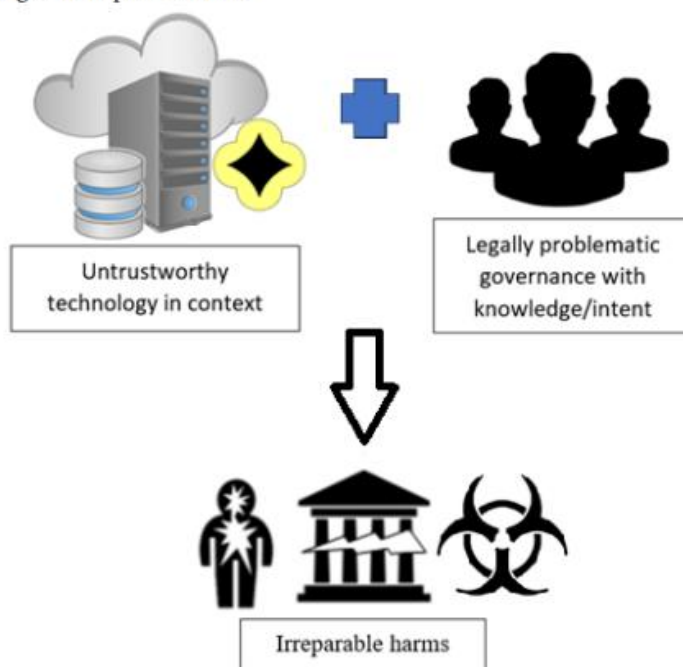
Author Summary of **EXPLOIT MACHINA**, 59 UC Davis L. Rev. 1635 (2026)

Full article: https://lawreview.law.ucdavis.edu/sites/g/files/dgvnsk15026/files/2026-03/59-3_Matwyszyn.pdf

1. Technology fraud prosecutions (e.g. Theranos, the Boeing MCAS system, the VW emissions defeat devices) and the last decade of government AI tool disasters point to a systemic technology safety problem: untrustworthy technologies are combining with broken governance structures to potentially irreparably harm human safety. Key technology and AI decisionmakers now regularly harm the public with knowledge or intent.
2. These situations feel like a form of insider attack to the harmed members of the public and the organizations that rely on these technologies. These scenarios are experienced as a betrayal of trust in a context where insiders have superior technical knowledge (about flaws) that they leverage that knowledge to the detriment of others.
3. This dynamic of broken tech plus broken governance deserves its own name – exploit machina. Exploit machina is the lodestar technology issue of the 21st century. Trustworthy tech cannot succeed in a market flooded by exploit machina technologies.

2026] *Exploit Machina* 1645

Figure 1: Exploit Machina



4. Exploit machina means that the flaws of hardware and software/ AI combine with the flaws of governance to potentially cause irreparable harms at scale. These harms are not only individual; they are also social in nature. Hannah Arendt warned us about this – she cautioned about an undesirable form of hyper-automation called “cybernation.” She warned us to “think what we are doing” because of the potentially corrosive impact of cybernation on democracy. Meanwhile, President Eisenhower warned us about the emergence of a scientific and technical elite that would threaten the national security of our country.
5. Exploit machina scenarios that feel like insider attacks have historical precedents. These are not new dynamics – confidentiality, integrity, and availability gaming using sensing technologies is a centuries-old problem. For example, the sensing technologies used in the Watergate tapes, witchcraft trials, forced sterilizations of “feebleminded” people, and NYC tuberculosis truck deployments in the 1960s, potentially all reflected early versions of exploit machina. Similarly, Congress and states regulated polygraph use in the private sector due to concerns over technology abuse and exploit machina.
6. The irreparable harms from exploit machina are damaging to both economic and mental health. The flaws of hardware and software in AI tools combine with the AI data processing backend that makes predictive and prescriptive judgments, databases that often contain stale or erroneous information.
 - a. The current generation of AI fosters reproductive rather than productive imagination – a distinction identified by (Arendt’s reading of) Kant. This deterioration toward lower quality thinking undercuts the future of an economy driven by human creativity.
 - b. These data flows are coming from increasingly privacy-intrusive spaces, such as in-cabin video and audio recording (and potential psychological profiling) of drivers and passengers in cars. In this way, a “digital evil twin” version of your identity (driven by the undisclosed KPIs of others) becomes created that is outside your control. This digital evil twin version can then preemptively lock you out of economic opportunities and the chance to better your life. It can also erode your ability to tell your own life story and to bounce back and reimagine your own future – a quintessential (and culturally specific) aspect of American life stories. Benjamin Franklin and developmental psychologists have explained the importance of this self-narration to our development. Again, this digital evil twin problem is experienced as an adversarial attack on identity.
7. Despite a quarter of a century of self-regulatory efforts, little meaningful progress has happened on technology safety AI adds to the urgency of addressing the underlying technology safety and computer security problems. The market is currently overwhelmed with noise from exploit machina fraud and low-quality tech, stifling its ability to reward and recognize technology built with safety and security as a priority.
8. Traditional industries are being eroded from the inside by exploit machina. Every company is a technology company now, relying on internal computerization and cloud storage. But traditional industries are held to meaningful liability standards, while technology companies are continuing to be a comparatively underregulated sector of the economy, despite sometimes imposing irreparable harms on other organizations and the public. This sets up a no-win situation for

traditional industries, where exploit machina may trigger liability for traditional companies but not apportion responsibility to the companies that engaged in the underlying exploit machina behaviors.

1776

University of California, Davis

[Vol. 59:1635]

Figure 3: Legal Governance by Product and Service Category

PRODUCT or SERVICE	SOCIAL HARM at scale possible?	TARGETED ENFORCEMENT AGENCY?	ENFORCEMENT/ PRIVATE LITIGATION
Technology	Yes – death, economic, national security	No dedicated federal agency; some state activity, limited professional self-organization (SROs)	Sporadic federal/state criminal/civil enforcement by government + suits by private litigants
Financial	Yes – economic, national security	Multiple federal and state + licensing, SROs	Federal and state criminal/civil + suits
Goods [traditional]	Yes – death	Federal, state, local + some licensing, SROs	Federal and state criminal/civil + suits
Power	Yes – death, economic, national security	Multiple federal, state + licensing, SROs	Federal and state criminal/civil + suits
Transport	Yes – death, economic, national security	Multiple federal, state + licensing, SROs	Federal, state, local criminal/civil + suit
Environmental	Yes – death, economic, national security	Federal, state, local + some licensing, SROs	Federal, state, local criminal/civil + suits
Consumables/food and drugs	Yes – death, economic, national security	Multiple federal, state, local + licensing, SROs	Federal, state, local criminal/civil + suits
Medical devices; healthcare	Yes – death, economic, national security	Multiple federal, state + licensing, SROs	Federal criminal/civil + suits
Communications	Yes – death, economic, national security	Federal, state + licensing, SROs	Federal and state criminal/civil, suits
Insurance	Usually not – economic	Multiple federal partial + State + licensing, SROs	Federal and state criminal and civil + suit
Construction	Usually not – death	Multiple federal partial + State + licensing, SROs	State criminal sanction, civil + suits
Body/ aesthetic enhancement	Usually not – death	State + licensing, SROs	Criminal, civil + suits
Legal; other professional/ trade services	Usually not	State + licensing, SROs	Criminal, civil suits
Arts and related professions	Usually not	Primarily SROs	Criminal, civil suits

9. The legal path forward is technology neutral: it focuses on three variables – Context and control, the Harm and its irreparability, and the Intent/knowledge of the technology builders and operators (“CHI”).
10. A two-pronged approach can implement these CHI variables:

(1) threat meta-modeling with an eye on insider threats and all impacted constituencies – something absent from current dominant models;

1768

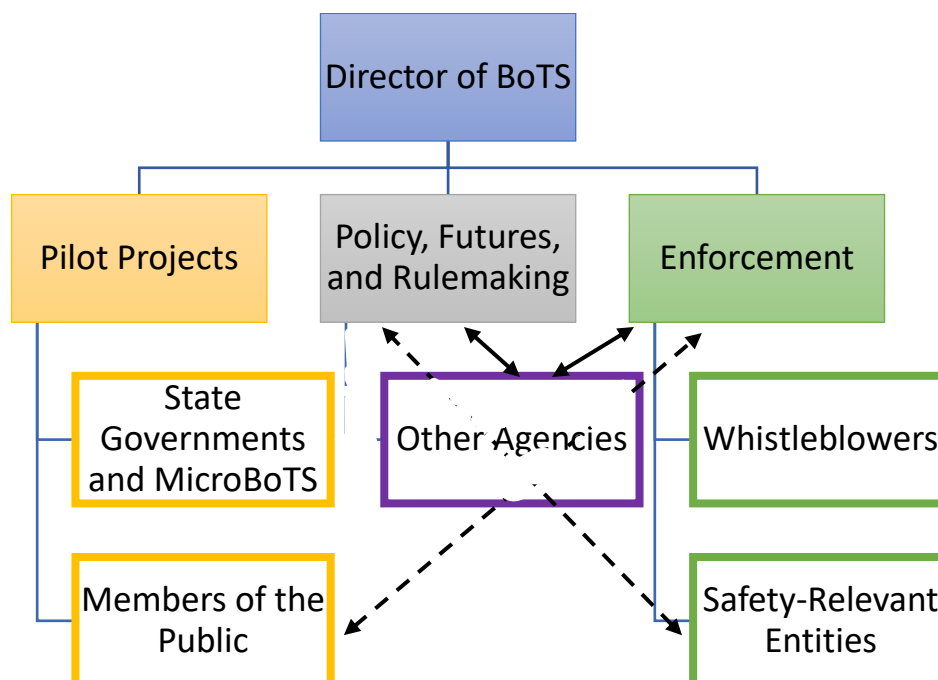
University of California, Davis

[Vol. 59:1635]

Figure 2: The TROL Threat Metamodel

<u>TROL</u>	<u>THREAT META-MODEL</u>
Technology:	Assess (1) organizational and (2) product specific assessments technical and operational risk using threat modeling methodologies most suitable for the organization per standards of the computer security community
Regularity:	Assess consistency, usability, and predictability of (1) technological and organizational response to problems identified by end users/members of the public and (2) product performance in light of sensitivity of foreseeable deployment contexts
Organization:	Assesses robustness of governance internal controls, oversight, and incident response structures in both (1) external attacker threat scenarios and (2) insider threats, including a corrupted officer or director.
Legal:	Assess potential harm to all foreseeable parties, not only to users/ investors

and (2) a new technology regulator of last resort, a **federal Bureau of Technology Safety (BoTS) with state corollaries (microBoTS)**. BoTS is a self-consciously novel model, a peer agency that assists others and fills gaps where needed; yet, it also remixes and expands upon elements that have worked successfully in other safety regulation contexts.



- BoTS would have three branches:
 - Pilot Projects: A community ombudsman to scale information sharing with state and local government + a (small) team to “future proof” the national tech economy with bottom-up community-led projects solving real problems; “Build the Future” contests and other bottom-up efforts; a domestic, safety-first “US of Tomorrow” tech incubator; computer security infrastructure tiger teams to help with updating and incident response, e.g. hospitals addressing ransomware crises.
 - Policy, Futures, and Rulemaking: Rulemaking focused on empowering market mechanisms in interstate commerce, 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. 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 BoTS’s disclosure-based filings –BoTS should have civil and criminal fining and injunctive authority; a tech safety whistleblower office to process tips from both inside and outside government.
- BoTS’s mission would focus on technology safety enhancement, safety baseline maintenance, and tech safety fraud.

- BoTS structure is a different “friendly expert” agency model that scales – driven by bottom-up technology reality for states and communities, as it impacts interstate commerce
 - State governments do not have a fair shot of keeping up with Big Tech policy/ maneuvers on a national level
 - Peer collaboration and gap filling across existing agencies + a technology regulator of last resort;
- BoTS is nimble, financially self-sustaining, entrepreneurial, and First Amendment sensitive by design;
- BoTS offers a technology neutral approach that will scale alongside future tech.
- BoTS can correct 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. For example, multiple agencies consider food safety, but zero are dedicated to tech safety.
 - Addresses rampant technology fraud that is hurting market mechanisms and honest businesses. BoTS would facilitate market recognition of safety-first tech companies.