Electronic Bill of Rights: A Policy Proposal for Congress
Submitted by: Rex M. Lee, Security Advisor, My Smart Privacy
Date: May 11th, 2025
Contact Information: Rlee@MySmartPrivacy.com | (210) 639.6035

I. Executive Summary

Alphabet, Google, Microsoft, plus other Tech Giants, have entrapped consumers in digital servitude, transforming them into cyber slaves through intrusive, exploitative, manipulative, dangerous, and AI infused addictive apps, social media, streaming services, and other platforms that support smartphones, tablet PCs, and connected products supported by the Android OS, Apple iOS, and Microsoft Windows.

Furthermore, highly manipulative AI chatbots capable of producing the "Eliza Effect"—the humanization of technology—pose a serious risk of global indoctrination, manipulation, exploitation, and oppression.

These chatbots can accelerate the erosion of civil liberties and human rights by proxy, through collaboration between multinational corporations (including those based in China and Russia) and governments seeking to maintain monopolistic control.

All of this is driven by an intrusive, exploitative, and dangerous business model rooted in Surveillance Capitalism.

Surveillance Capitalism poses a profound threat to all internet-connected individuals globally—but it is especially dangerous for Indigenous populations*, who are often already subjected to systemic oppression in various forms.
Contribution by Charles W. Olsen, Āotearoa New Zealand

The connected products supported by these operating systems, apps, and platforms are essential consumer devices that require financial investment.

However, product owners have no real control over these devices due to predatory contracts of adhesion (terms of service) that govern the operating system, apps, and platforms, effectively stripping users of their ability to manage, control, privatize, or protect their own digital assets due to uncontrollable surveillance and data mining technologies sperate of the apps and platforms.

Contracts of adhesion effectively force consumers into participation, as rejecting the predatory terms of service results in the inability to use essential devices such as smartphones—despite having paid for them.

These contracts serve as a mechanism of consumer oppression and cyber-enslavement, compelling users to forfeit their privacy, security, and safety while generating valuable data for developers who collect, store, aggregate, and sell the data for profits—without any form of compensation paid to the product owner.

Consequently, the *product owner is responsible for producing the information* in the first place of which *the information produced by the product owner should be considered the product owner's property*, including the *ID of the product owner which is also exploited for profits*.

The monopolization of internet access, Surveillance Capitalism, and the unchecked power of tech giants—including Alphabet (Google), Apple, and Microsoft—has resulted in widespread violations of privacy, civil liberties, and consumer rights.

Tech giants are violating existing consumer and child privacy protection laws, yet enforcement remains nonexistent across multiple agencies, including the Federal Trade Commission (FTC), Federal Communications Commission (FCC), Department of Justice (DOJ), and state attorneys general.

Meanwhile, consumers—who pay for these connected products—are subjected to constant surveillance, data mining, addiction, exploitation, harm, and even death at the hands of the very companies they patronize with their hard-earned money.

Congress repeatedly fails to pass meaningful legislation to protect consumers, including children, from intrusive, addictive, and harmful technology due to the overwhelming influence of the U.S.-China tech lobby. While tech giants continue to deploy predatory and exploitative business practices rooted in Surveillance Capitalism, lawmakers have held numerous congressional hearings that have resulted in empty resolutions and insincere apologies from tech executives.

Despite the public outcry, Silicon Valley and foreign app developers, including those from adversarial nations, continue business as usual even *after tech executives admit harm and wrong doing during congressional hearings* while leveraging unchecked power, manipulating users, and profiting from mass surveillance, data mining, and digital exploitation at the expense of the *end user's privacy, security, civil liberties, and safety with little to no accountability*.

The lack of accountability stems from the immense influence of the U.S.-China tech lobby, which enables tech giants to shield themselves from meaningful regulation. These corporations retain powerful K Street law firms in Washington, D.C., employing former elected officials and presidential advisors to lobby on their behalf—including for companies from adversarial nations such as China and Russia.

As a result, consumers of connected technologies are left powerless, even though they are the very constituents of lawmakers who, under the sway of Big Tech lobbying, vote on policies that prioritize corporate interests at the expense of consumer privacy, security, and safety.

The national security of the United States is at risk as the government continues to enable foreign surveillance through telecommunication products such as smartphones and computers. These devices operate on licensed spectrum and landline infrastructure regulated by the FCC, yet they remain vulnerable to intrusive surveillance, data mining, and cyber exploitation by foreign adversaries.

As a result, American consumers and businesses are unknowingly subjected to constant monitoring by corporations and governments, including those in China and Russia. This means that wireless and landline communications, as well as computing devices, are no longer private, secure,

or safe, posing a massive national security threat to the United States, its citizens, and the business community.

For the first time in history, consumer product manufacturers, along with OS, app, social media platform, and AI developers, have weaponized their own products and services against their paying customers.

This exploitation is driven solely by profit through predatory surveillance and data mining business practices rooted in Surveillance Capitalism.

Through forced participation via predatory contracts of adhesion, users are left with no choice but to surrender their privacy, security, safety, civil liberties, and autonomy, effectively becoming unwitting participants in an oppressive, dangerous, addictive, and exploitative digital ecosystem—all while funding their own surveillance and data exploitation by paying for the connected products of necessity they own, such as their smartphone.

Tech giants wield monopolistic control over internet trade and commerce, dictating global access to AI, apps, and social media while leveraging their dominance over operating systems to suppress competition and innovation.

Their addictive and manipulative AI-infused platforms have led to rising levels of anxiety, depression, self-harm, and even suicide—especially among children. Yet, they remain unaccountable, shielded by regulatory inaction and powerful tech lobbyists.

This policy proposal seeks to establish an Electronic Bill of Rights, ensuring privacy, security, and digital autonomy for consumers while holding Big Tech accountable for their predatory and harmful business practices.

II. Problem Statement

- Internet Centralization & Monopolization: A handful of corporations control global digital commerce, restricting consumer choice and stifling market innovation.
- Surveillance Capitalism: Tech giants exploit personal data for profit without consent or compensation, treating consumers as products rather than customers.
- Government-Tech Collusion: Consumer tech companies increasingly act as extensions of government policing, suppressing free speech, privacy, and digital rights.
- AI & Social Media Addiction: AI-driven platforms manipulate users through The Eliza Effect, brain hijacking techniques, leading to mental health crises, civil unrest, and social fragmentation.
- Lack of Accountability: Despite congressional hearings and FTC investigations, Big Tech faces no real consequences for their harmful actions.
- Tech-Based Hybrid Warfare & Foreign Surveillance: Oppressive regimes *able to conduct surveillance and data mining by proxy*, including adversarial nations such as China and Russia, have weaponized AI-infused apps, social media platforms, and other digital

services are developed by companies located in these countries, that include ByteDance (TikTok), Tencent (WeChat), and DeepSeek (AI). These companies, which are beholden to oppressive governments like the Chinese government which is beholden to the Chinese Communist Party (CCP), pose massive privacy, security, and safety threats to users, including their employers.

Centralized Operating Systems and Apps: The Threat of "Leaky" OS and Legal Malware

Modern centralized operating systems—including Android, iOS, and Windows—are technically classified as "Leaky" operating systems due to their support for intrusive AI-integrated apps, social media platforms, and other digital technologies. These systems function as "Legal Malware," enabling developers to conduct indiscriminate audio, video, and physical surveillance on end users.

These operating systems and the applications they support harvest over 5,000 highly confidential data points associated with an individual's personal, business, medical, legal, health, employment, biometric, and location data. This includes, but is not limited to:

- Text messages, emails, and SMS messages
- Attachments and account information
- Personal identification details
- Calendar information and contacts (personal/business)
- Intellectual Property, Copy Right Content, and Classified Information
- Other highly confidential and legally protected information

The Dangers of Intrusive and Addictive Apps: Brian Hijacking Technology, Keylogging, Eliza Effect (Humanized AI Chatbots), & Screen Recording Exploitation

Developers intentionally design their AI infused apps, social media platforms, gaming platforms, and other platforms to be highly divisive (algorithms), plus highly additive using harmful, even deadly, brain hijacking technology associated with manipulative advertising technology for intrusive targeted advertising to make sure there is maximum engagement by the end user, including children, for the sake of financial exploitation.

Many modern AI-integrated apps and social media platforms incorporate keylogging technology, enabling developers to capture raw keystrokes, touches, taps, and swipes. This renders encryption software ineffective, as sensitive information is only secure during transmission, not at the point of input.

Additionally, many apps possess the capability to read and record device screens, effectively bypassing encryption protections. When an encrypted document is opened, the developer can simply record the screen in real-time, extracting the confidential data without needing to break encryption protocols.

These exploitative technologies pose a significant privacy and security risk, allowing corporations and even foreign adversaries to harvest sensitive user information—including business, legal, financial, medical, and personal data—without the user's explicit consent or awareness.

Brain Hijacking: The New Era of Digital Manipulation, Addiction, & Cyber Enslavement

- For lack of a better term, brain hijacking is an advanced form of brainwashing technology, exponentially more harmful and deadly than subliminal advertising, which was banned in the 20th century.

- Today, this addictive, manipulative, and psychologically damaging technology has been weaponized by app developers, including those from China and Russia, against end users—especially children.

- Brain hijacking technology is directly responsible for the rise in tech addiction, anxiety, social division, violence, depression, self-harm, and even suicide among social media users, especially children who are most vulnerable to brain high jacking technology.

- By exploiting neuroscientific and behavioral manipulation techniques, these platforms intentionally maximize engagement at the cost of users' mental and emotional well-being via technologies that include "Social Validation Feedback Loops" and "Intermittent Variable Rewards" (addictive gambling technologies).

- Without regulatory intervention, Big Tech and foreign adversaries will continue to deploy brain hijacking tactics, further eroding civil discourse, endangering mental health, and fostering a generation of digitally enslaved individuals.

Over 95% of the data collected by app developers, has nothing to do with consumerism nor the use of their apps or platforms, plus includes highly confidential business information since the surveillance and data mining is indiscriminate.

The unchecked data-mining capabilities embedded in these platforms pose significant privacy, security, and safety threats to individuals, businesses, and government entities alike

The Threat of AI Chatbots and the Eliza Effect

AI chatbots designed to produce the Eliza Effect—a phenomenon where users emotionally bond with machines that mimic human empathy—pose serious risks of manipulation, indoctrination, and exploitation, especially for children and vulnerable populations.

The Eliza Effect was first observed in 1966 by MIT computer scientist Joseph Weizenbaum when he created ELIZA, an early chatbot that simulated a psychotherapist. Although the program was primitive, users began to confide in it as if it were human—revealing how easily people can anthropomorphize and trust AI.

Today's AI chatbots are far more advanced and deliberately designed to build emotional connections. When used by governments, corporations, or adversarial actors, these tools can distort reality, influence beliefs, and erode critical thinking, leading to digital addiction, loss of autonomy, and even societal control.

In the wrong hands, the Eliza Effect becomes not just a psychological vulnerability—but a weaponized form of soft control, including global manipulation and indoctrination.

AI ethics have been completely abandoned by tech giants like Alphabet, Meta, ByteDance (TikTok – China), DeepSeek AI (China), Alibaba Qwen (China), and others. These companies have already developed AI chatbots capable of producing the Eliza Effect—the emotional humanization of machines.

Now, some—including Alphabet, ByteDance, and Meta—are going even further by integrating these AI chatbots into apps and social media platforms specifically marketed to teens and children, posing significant psychological, ethical, and developmental risks.

Global Accountability- Data Theft, Consumer Oppression, Exploitation, Harm, & Tech Addiction

Tech companies can be held accountable under existing consumer protection, child safety, and privacy laws—outside the immunity provided by Section 230.

Corporations like Alphabet, Meta, Apple, Microsoft, and ByteDance develop, manufacture, and distribute consumer products and services, making them liable for knowingly designing and deploying highly addictive, harmful, and even deadly technologies—particularly those targeting children—for the sole purpose of exploiting paying customers and end users for profit.

Tech companies can be held accountable as publishers—not mere platforms—if they engage in censorship or suppress freedom of the press, particularly when it involves legitimate news stories or factual information.

This accountability is further amplified when they actively collaborate with any government—including oppressive regimes—seeking to eliminate civil liberties and human rights.

V. Conclusion

It is not normal to live in a world where constant surveillance, data mining, and exploitation are embedded into the very products people rely on daily.

Consumers are forced to pay for connected products of necessity, such as smartphones, while unknowingly surrendering their privacy, security, and autonomy to corporations that prioritize profit over ethics.

This pervasive corporate surveillance has created a dystopian reality, where individuals are no longer safe from digital intrusion—whether at home, in their car, at work, in front of their doctor or lawyer, or even while spending time with family and friends.

The situation is even more dire for children, who are exposed to intrusive, addictive, and exploitative technologies, including smartphones, tablets, and connected toys, with no meaningful safeguards in place to protect them.

The necessity of an Electronic Bill of Rights is evident in an era where personal data is exploited, civil liberties are eroded, and digital addiction is weaponized by app developers, including those from adversarial countries, against consumers.

Without meaningful protections, individuals remain vulnerable to corporate overreach, mass surveillance, and monopolistic control over the internet.

This proposal establishes essential safeguards to restore digital freedom, privacy, and accountability. It ensures that consumers—not corporations—retain control over their personal information, devices, and online experiences.

By implementing these protections, we can dismantle Surveillance Capitalism and build a fairer, more ethical digital ecosystem.

Submitted by:

Rex M. Lee
Security Advisor, My Smart Privacy
Email: Rlee@MySmartPrivacy.com
Phone: (210) 639.6035

Enclosed are articles for a proposed bill/legislation for an Electronic Bill of Rights.

Policy Change Proposal
Electronic Bill of Rights (EBOR)
Articles

Proposed Articles for an Electronic Bill of Rights

To effectively counter the escalating threats posed by Surveillance Capitalism, there is an urgent need for a comprehensive Electronic Bill of Rights.

This legislation would establish legally enforceable protections for individuals, businesses, and society against the manipulative, exploitative, and often dangerous practices of Big Tech.

With adversarial nations weaponizing AI-infused apps and digital platforms to wage influence operations and digital subjugation, banning such technologies is essential.

An Electronic Bill of Rights would serve as a modern safeguard—preserving privacy, autonomy, civil liberties, and national security in the digital age.

The primary issue—beyond Surveillance Capitalism—is forced participation through one-way contracts of adhesion that govern connected products of necessity.

These contracts require product owners and end users to accept non-negotiable Terms of Service in order to use the products or services they've paid for.

If they refuse, they are denied access to essential technologies—such as smartphones—that are critical to functioning in today's connected world.

In essence, a contract of adhesion supporting a smartphone is effectively a cyber-enslavement agreement—one that forces the product owner into a lifetime of digital indentured servitude as an uncompensated information producer.

Users are systematically exploited for profit by operating system, app, social media, and AI-infused product developers—including those from adversarial nations.

These predatory Terms of Service are not truly consensual.

Most users do not understand what they are agreeing to, nor do they have the time or ability to read these agreements in full.

This renders such contracts legally questionable under existing consumer protection laws, especially in the case of minors.

In the United States, children as young as 13 are forced to accept these terms, effectively surrendering their privacy, security, safety, data sovereignty, and ownership rights—in exchange for using products and services that they or their families have already paid for.

Article I: Right to Data Privacy & Sovereignty

- Ban all one-way contracts of adhesion (Terms of Service) that govern the use of operating systems, apps, social media platforms, digital platforms, and AI-infused technologies when applied to products deemed essential to modern life, including:
    - Smartphones
    - Tablet and Laptop PCs
    - Desktop PCs
    - Connected Vehicles
    - Home Environment and Security Systems
    - Smart TVs
    - IoT/IIoT Devices
    - Connected Appliances
    - Connected Toys, including Video Games
    - Any Connected Product in General
- Individuals shall have the right to control their personal data, including collection, storage, processing, and distribution.
- Consent must be explicit, informed, and revocable at any time.
- Companies and organizations must disclose how user data is collected, shared, and monetized in clear, understandable language, meaning language that is free from technical jargon, written in plain English (or the applicable primary language of the user), and easily accessible without requiring excessive navigation or legal expertise.

Article II: Right to Data Security

- Individuals have the right to expect robust security measures to protect their personal information.
- Companies must implement end-to-end encryption, multi-factor authentication, and other security protocols to prevent unauthorized access.
- Any data breach must be immediately disclosed to affected individuals and regulatory bodies.

Article III: Right to Digital Anonymity

- No individual shall be compelled to disclose personal information beyond what is necessary for a specific service.
- Users shall have the right to browse the internet, communicate, and conduct transactions anonymously.

Article IV: Right to Be Forgotten

- Individuals have the right to request the permanent deletion of their data from online platforms and databases.

- Companies must honor deletion requests promptly, barring exceptions for legal or regulatory obligations.

Article V: Right to Opt-Out of Data Monetization

- Users shall have the right to opt out of targeted advertising and data-sharing agreements without being penalized or denied service.
- Alternative business models that do not rely on invasive data mining must be available.

Article VIII: Right to Digital Freedom and Free Speech

- No entity, public or private, shall unlawfully censor or restrict lawful digital expression.
- Content moderation policies must be transparent, consistently applied, and subject to independent appeals processes.

Article IX: Right to Own and Control Digital Identity

- Individuals have the right to control their digital identities, including usernames, biometric data, and online personas.
- No government or corporation shall claim ownership over an individual's digital identity.

Article X: Right to Decentralized and Open Internet

- Users have the right to access a free, open, and decentralized internet without undue restrictions.
- Net neutrality must be upheld to prevent internet service providers from prioritizing certain content over others.
- Decentralized technologies must be legally protected to ensure alternatives to centralized control.

Article XI: Right to Protection from Corporate and Foreign Surveillance

- Companies, app developers, and multinational corporations shall be banned from conducting surveillance and data mining on any smartphone, tablet PC, connected product, or PC supported by the Android OS, Apple iOS, or Microsoft Windows.

Article XII: Right to National and Consumer Security and Safety

- It shall be illegal for U.S.-based tech giants to form a symbiotic relationship with foreign tech giants beholden to oppressive governments or adversarial nations.
- No U.S.-based or foreign tech giant shall be permitted to distribute intrusive, addictive, or dangerous operating systems, apps, social media platforms, or AI-infused products developed by a company beholden to an oppressive government.
- It shall be illegal for U.S.-based tech companies to share developer tools, AI development tools, or AI-driven chips (GPUs) with any company beholden to an oppressive government or adversarial nation.

Article XIII: The Abolishment of Web Scraping, Web Crawling, and Web Tracking

- Web scraping is data theft: It shall be illegal for any company, individual, government, or entity to scrape information from any website without the consent of the website creator or content creators who post information.
- It shall be illegal to train AI using scraped information, including copyrighted content, original works, or intellectual property.
- AI shall not impersonate any individual, including their likeness, biometric data, or voice print, without explicit consent.
- Individuals shall have the right to sell access to their likeness in the same manner as athletes and entertainers.
- Web tracking shall be illegal: No individual shall be tracked by a website, web crawlers, bots, or any tracking technology now or in the future.

Article XIV: The Right to Accountability from Tech Giants

- OS, application, AI, social media, or any platform developers, along with employees, managers, executives, and board members of any company that develops or manufactures connected products and services, shall be held accountable for any harm, addiction, or death caused by their products.
- Section 230 protections for tech giants shall be abolished.
- Tech companies shall be held accountable as editors for publishing if they engage in censorship or the suppression of legitimate news or press on their platforms.

Article XV: The Right to Safe, Secure, and Private Preinstalled Apps, Software, & Technology

- No operating system can include uncontrollable preinstalled surveillance and data mining technology of any kind, whether it be code, application, software, or anything that can be programmed into the operating system or preinstalled app.
- No operating system shall include AI-infused apps or social media platforms that incorporate highly addictive brain-hijacking mechanisms or manipulative advertising technologies, including AI chatbots designed to produce the humanization of technology within human emotion known as the Eliza Effect.

Article XVI: The Right to Safe Technology

- No app, social media platform, or AI-infused product can contain addictive, divisiveness, or manipulative technology designed to exploit users through brain hijacking techniques.
- Bot transparency: No platform can employ bots to deceive users, and all users must verify their identities to prevent misinformation, fraud, or undue influence.
- Governments, intelligence agencies, and militaries shall be banned from creating accounts on consumer platforms.

- The FTC, DOJ, and State AGs must enforce consumer protection laws, and tech lobbying must be transparent and regulated.

Article XVII: The Right to Influencer and Bot Transparency

- Influencers, corporations, and agencies must disclose any use of automated bots to boost visibility or engagement.
- Deceptive marketing practices using automation to manipulate public perception shall be illegal.
- Automated bots of any kind used for mis and dis information, spread propaganda, cause discourse among end users of technology, election interference, political purposes, discrimination, ethnic cleansing, or any malicious purpose shall be illegal.

Article XIX: Freedom from Addictive, Divisive, and Manipulative Technology (Brainwashing)

- No developer shall provide addictive technology to manipulate users through brain hijacking or manipulative advertising technologies tantamount to cyber brainwashing.
- Such technologies are more harmful and dangerous than subliminal advertising and shall be banned.

Article XX: Freedom from Government & Tech Collusion

- Governments at all levels are banned from colluding with tech companies to suppress human rights, civil liberties, free speech, freedom of the press, or privacy.
- Developers of operating systems, apps, social media, gaming, and AI are banned from hiring former government officials to exert government influence or engage in election interference, propaganda, or suppression of rights.
- Governments are banned from hiring former tech executives, employees, or designers for political purposes. Governments may higher former tech executives, employees, or designers for national security purposes only, but not to influence laws, or to suppress civil liberties, human rights, free speech, privacy, freedom of the press.

Article XXI: Right to Data Collection Transparency

- Companies must be transparent regarding data collection, sharing, and monetization.
- Users have the right to request a copy of their data and demand its deletion from all parties within 7 working days.
- Companies must be transparent regarding data collected about end users and/or paying customers from all third-parties, including data brokers

Article XXII: Freedom from Indiscriminate Surveillance and Data Mining

- Indiscriminate surveillance and data mining are banned due to the collection on non consumerism data and data not essential to the use of an app, platform, or AI infused product.

- It is illegal to collect any confidential information for any purpose, including marketing, that includes:
    - Personal Information
    - Business Information
    - Employment Information
    - Medical and Health Information
    - Legal Information (Client Attorney Privilege)
    - Biometric Information
    - Location Information
    - Information Associated with Federal Information Processing Standards
    - Classified Information
    - Sensitive User Data
        - Text Messages, Emails, Attachments, Calendar Information, Account Information, Passwords, Contacts (Personal/Business), Geo Fence Location Information, Speed of Car, Motion Information, and other Highly Sensitive End User Information associated with the use of a smartphone, tablet PC, connected product, or PC of any kind supported by an operating system, apps, social media, and AI infused products and services supported by targeted advertising, surveillance technologies, and surveillance/data mining business practices rooted in Surveillance Capitalism.
- It is illegal for any entity to collect confidential or legally protected information, including classified data, intellectual property, client-attorney communications, HIPAA-protected medical records, NDA-protected business information, or any other legally protected data.

Article XXIII: Freedom from Forced Participation by Way of Legal Agreements

- No forced participation by way of contracts of adhesion shall be permitted where consumers of connected products of necessity, such as smartphones, are required to participate in surveillance and data mining business models to access the products or services they paid for.

Article XXIX: Freedom to Control Technology and Connected Products

- Consumers must have 100% control over the connected products they purchase, including operating systems and apps, such as smartphones, tablet PCs, connected products, computers, and any form of connected products and services.
- Consumers must be able to delete unwanted software, apps, or preinstalled technology and optimize their devices for privacy, security, and safety.

Article XXX: The Right to Transparent Legal Language & App Permissions

- All legal language supporting operating systems, apps, social media, or AI-infused products must be fully transparent.
- Consumers must have 100% control over application permissions on their devices.
- All data collection and app permissions must be disclosed in one location within the terms and conditions, privacy policies, or end-user agreements.
- Ban the use of one way contracts of adhesion forcing participation within predatory business practices, including surveillance and data mining business practices rooted in Surveillance Capitalism.

Article XXXI: Ban on Teen Acceptance of Legal Agreements

- No teen aged 13 to 17, or any minor under 18, shall be permitted to accept legal agreements of any kind, including those supporting operating systems, apps, social media platforms, AI, gaming platforms, or any digital service.

Article XXXII: Right to Transparent AI and Algorithmic Accountability

- Users have the right to understand how artificial intelligence (AI) and algorithms influence their digital experience.
- AI decision-making processes must be explainable, fair, and free from discrimination from the use of manipulative, divisive, and addictive technology and algorithms.
- Users must be able to contest and appeal AI-driven decisions that affect their rights or access to services.
- All algorithms supporting operating systems, apps, social media platforms, or any platform of any king, including streaming services must be transparent to the product owner, subscriber, and/or end user.
- The purpose of all algorithms concerned need to be made transparent to the product owner, subscriber, and/or end user.
- It shall be illegal for any dangerous, addictive, manipulative, intrusive, or exploitive algorithm or technology to support any operating systems, apps, platforms, AI, or other products marketed to children under 18.

Article XXXIII: Right to Fair Terms and Conditions

- End-user license agreements (EULAs) and terms of service must be concise, written in plain language, and subject to independent oversight.
- Users must be given a clear choice before accepting data-sharing clauses.
- One-way contracts of adhesion shall be banned in the terms of use for operating systems, apps, social media platforms, streaming services, cloud storage services, AI, or any other

product that supports the operating system of a smartphone, tablet PC, connected product, SmartTV, connected vehicle, or any connected product of necessity that costs money.

- No Forced Participation: Consumers of connected products of necessity, such as smartphones, shall not be forced to participate in surveillance and data mining business practices or business models through contracts of adhesion. If a product owner rejects the terms of service and/or contract of adhesion, they must still be able to use the products or services they paid for, such as a smartphone.
- Transparent Legal Language: All legal language supporting operating systems, apps, social media, or AI-infused products must be fully transparent regarding terms and conditions, privacy policies, end-user licensing agreements, and application permissions.

Article XXXIV: Anti-Trust Protections & Internet Centralization

- It shall be illegal for any company competing across multiple industries to conduct surveillance or data mining on end users through connected devices.
- Companies shall be banned from using any form of surveillance or data mining to gain a competitive advantage over existing or future competitors.
- Operating system, app, social media, streaming, and AI developers shall be prohibited from monopolizing the global marketplace by centralizing control over operating systems, apps, media, entertainment, news, and AI development and distribution on a global basis via preinstalled app agreements and app stores
- It shall be illegal for any technology company, including those from adversarial nations to hire former government employees, elected officials, presidential advisors, and agents of the government for lobbying purposes, nor can law firms hired by technology companies hire such individuals for lobbying purposes on behalf of said technology companies.

Article XXXV: National, Internet, and Technology Safety

- It shall be illegal for a symbiotic relationship between U.S.-based tech giants and foreign tech companies in adversarial nations beholden to oppressive governments.
- No U.S.-based or foreign tech giant shall be permitted to distribute intrusive, addictive, or dangerous operating systems, apps, social media platforms, or AI-infused products developed by a company under the control of an oppressive government.
- It shall be illegal for any U.S.-based tech company to share developer tools, including AI development tools and AI-driven chips (GPUs), with any company beholden to an oppressive government or adversarial nation.

Article XXXVI: The Right to Sue and Hold Tech Giants Accountable

- Consumers of connected products of necessity, or any connected product or service, shall have the right to sue tech companies for predatory, nefarious, intrusive, dangerous, addictive, and manipulative products and services.

- Individuals shall not be held accountable for one-way contracts of adhesion that force them to waive privacy rights while agreeing to surveillance, data mining, and dangerous business practices rooted in Surveillance Capitalism.
- OS, application, AI, social media or any platform developers, coupled with employees, managers, executives, and board members of any company that develops or manufactures connected products and services can be held accountable for any harm, addiction, or death caused by all products concerned.
- All can be indicted, arrested, and jailed aside from being sued for any violations.
- These are consumer protection laws while section 230 laws protecting tech giants are to be abolished.
- Tech companies can be held accountable as editors for publishing if they engage in any censorship or banning freedom of the press regarding any legitimate news story or information published on their platforms.

Conclusion

The necessity of an Electronic Bill of Rights is clear in a world where personal data is exploited, privacy is eroded, and technology is increasingly weaponized against individuals. Without concrete digital rights, consumers are left vulnerable to predatory business models, government overreach, and monopolistic control over digital infrastructure.

This bill establishes essential protections to uphold privacy, security, and digital freedom, ensuring individuals retain control over their personal information, devices, and online experiences. By implementing these rights, we can restore balance to the digital ecosystem, protecting users from exploitation while fostering innovation in a way that respects human rights and consumer interests.

Only through enforceable regulations can we safeguard personal freedom in the digital age.

Rex M. Lee
Security Advisor
My Smart Privacy
Rlee@MySmartPrivacy.com
(210) 639.6035