

1 AN ACT relating to protection of information and declaring an emergency.

2 *Be it enacted by the General Assembly of the Commonwealth of Kentucky:*

3 ➔Section 1. KRS 42.722 is amended to read as follows:

4 As used in KRS 42.720 to 42.742:

- 5 (1) "Artificial intelligence" means a set of technologies that enables machines to
6 perform tasks under varying and unpredictable circumstances that typically
7 require human intelligence or oversight, or that can learn from experience and
8 improve performance;
- 9 (2) "Artificial intelligence system" means a machine-based computing system that:
10 (a) Is built upon algorithms that can operate under varying circumstances
11 autonomously without human intervention;
12 (b) Is built on technology designed to simulate human intelligence;
13 (c) Operates by making observations about environments or data to make
14 predictions and decisions that affect real or virtual environments; and
15 (d) Is capable of learning from its experiences and improving its capabilities;
- 16 (3) "Communications" or "telecommunications" means any transmission, emission, or
17 reception of signs, signals, writings, images, and sounds of intelligence of any
18 nature by wire, radio, optical, or other electromagnetic systems, and includes all
19 facilities and equipment performing these functions;
- 20 (4) "Consequential decision" means any decision that has a material, significant, or
21 legal effect on providing or denying services, cost, or terms to any citizen or
22 business;
- 23 (5) "Deployer" means any department, agency, and administrative body that deploys
24 or uses a high-risk artificial intelligence system;
- 25 (6) "Developer" means any department, agency, or administrative body that develops
26 or intentionally and substantially modifies a high-risk artificial intelligence
27 system that is offered, purchased, sold, leased, given, or otherwise provided to

1 citizens and businesses in the Commonwealth;

2 (7) "External artificial intelligence system" means artificial intelligence systems that
3 are used to:

4 (a) Analyze data about individual citizens or businesses within the
5 Commonwealth;

6 (b) Make decisions relating to such individual citizens or businesses; or

7 (c) Produce outputs directly accessible by such individual citizens or
8 businesses;

9 (8) "Foundation model" means a machine learning model that is trained on broad
10 data at scale, designed for generality of output, and can be adapted to a wide
11 range of distinctive tasks;

12 (9) "General-purpose artificial model" means any form of artificial intelligence
13 system that displays significant generality, is capable of performing a wide range
14 of distinct tasks, and can be integrated into a variety of subsequent applications
15 or systems;

16 (10) "Generative artificial intelligence system" means any artificial intelligence
17 system or service that incorporates generative artificial intelligence;

18 (11)(2) "Geographic information system" or "GIS" means a computerized database
19 management system for the capture, storage, retrieval, analysis, and display of
20 spatial or locationally defined data;

21 (12) (a) "High-risk artificial intelligence system" means any artificial intelligence
22 system that is a substantial factor in the decision-making process or
23 specifically intended to autonomously make a consequential decision.

24 (b) "High-risk artificial intelligence system" does not include a system or
25 service intended to perform a procedural task, improve the result of a
26 completed human activity, or detect decision-making patterns or deviations
27 from previous decision-making patterns and is not meant to replace or

1 influence human assessment without human review, or perform a
2 preparatory task in an assessment relevant to a consequential decision;

3 ~~(13)~~~~[(3)]~~ "Information resources" means the procedures, equipment, and software that
4 are designed, built, operated, and maintained to collect, record, process, store,
5 retrieve, display, and transmit information, and associated personnel;

6 ~~(14)~~~~[(4)]~~ "Information technology" means data processing and telecommunications
7 hardware, software, services, supplies, facilities, maintenance, and training that are
8 used to support information processing and telecommunications systems to include
9 geographic information systems;

10 ~~(15)~~ "Internal artificial intelligence system" means artificial intelligence systems that
11 are only used internally by departments, agencies, and administrative bodies to
12 increase efficiency, streamline internal processes, or otherwise improve the way
13 such organizations function internally;

14 ~~(16)~~ "Machine learning" means the development of algorithms to build data-derived
15 statistical models that are capable of drawing inferences from previously unseen
16 data without explicit human instruction;

17 ~~(17)~~~~[(5)]~~ "Personal information" has the same meaning as in KRS 61.931;

18 ~~(18)~~~~[(6)]~~ "Project" means a program to provide information technologies support to
19 functions within an executive branch state agency, which should be characterized
20 by well-defined parameters, specific objectives, common benefits, planned
21 activities, expected outcomes and completion dates, and an established budget with
22 a specified source of funding;

23 ~~(19)~~~~[(7)]~~ "Security breach" has the same meaning as in KRS 61.931; and

24 ~~(20)~~~~[(8)]~~ "Technology infrastructure" means any computing equipment, servers,
25 networks, storage, desktop support, telephony, enterprise shared systems,
26 information technology security, disaster recovery, business continuity, database
27 administration, and software licensing.

1 ➔Section 2. KRS 42.726 is amended to read as follows:

- 2 (1) The Commonwealth Office of Technology shall be the lead organizational entity
3 within the executive branch regarding delivery of information technology services,
4 including application development and delivery, and shall serve as the single
5 information technology authority for the Commonwealth.
- 6 (2) The roles and duties of the Commonwealth Office of Technology shall include but
7 not be limited to:
- 8 (a) Providing technical support and services to all executive agencies of state
9 government in the application of information technology;
- 10 (b) Assuring compatibility and connectivity of Kentucky's information systems;
- 11 (c) Developing strategies and policies to support and promote the effective
12 applications of information technology within state government as a means of
13 saving money, increasing employee productivity, and improving state services
14 to the public, including electronic public access to information of the
15 Commonwealth;
- 16 (d) Developing, implementing, and managing strategic information technology
17 directions, standards, and enterprise architecture, including implementing
18 necessary management processes to ensure full compliance with those
19 directions, standards, and architecture;
- 20 (e) Promoting effective and efficient design and operation of all major
21 information resources management processes for executive branch agencies,
22 including improvements to work processes;
- 23 (f) Developing, implementing, and maintaining the technology infrastructure of
24 the Commonwealth and all related support staff, planning, administration,
25 asset management, and procurement for all executive branch cabinets and
26 agencies except:
- 27 1. Agencies led by a statewide elected official;

- 1 2. The nine (9) public institutions of postsecondary education;
- 2 3. The Department of Education's services provided to local school
- 3 districts;
- 4 4. The Kentucky Retirement Systems, the County Employees Retirement
- 5 System, the Kentucky Public Pensions Authority, and the Teachers'
- 6 Retirement System;
- 7 5. The Kentucky Housing Corporation;
- 8 6. The Kentucky Lottery Corporation;
- 9 7. The Kentucky Higher Education Student Loan Corporation; and
- 10 8. The Kentucky Higher Education Assistance Authority;
- 11 (g) Facilitating and fostering applied research in emerging technologies that offer
- 12 the Commonwealth innovative business solutions;
- 13 (h) Reviewing and overseeing large or complex information technology projects
- 14 and systems for compliance with statewide strategies, policies, and standards,
- 15 including alignment with the Commonwealth's business goals, investment,
- 16 and other risk management policies. The executive director is authorized to
- 17 grant or withhold approval to initiate these projects;
- 18 (i) Integrating information technology resources to provide effective and
- 19 supportable information technology applications in the Commonwealth;
- 20 (j) Establishing the central statewide geographic information clearinghouse to
- 21 maintain map inventories, information on current and planned geographic
- 22 information systems applications, information on grants available for the
- 23 acquisition or enhancement of geographic information resources, and a
- 24 directory of geographic information resources available within the state or
- 25 from the federal government;
- 26 (k) Coordinating multiagency information technology projects, including
- 27 overseeing the development and maintenance of statewide base maps and

- 1 geographic information systems;
- 2 (l) Providing access to both consulting and technical assistance, and education
- 3 and training, on the application and use of information technologies to state
- 4 and local agencies;
- 5 (m) In cooperation with other agencies, evaluating, participating in pilot studies,
- 6 and making recommendations on information technology hardware and
- 7 software;
- 8 (n) Providing staff support and technical assistance to the Geographic
- 9 Information Advisory Council and the Kentucky Information Technology
- 10 Advisory Council;
- 11 (o) Overseeing the development of a statewide geographic information plan with
- 12 input from the Geographic Information Advisory Council;
- 13 (p) Developing for state executive branch agencies a coordinated security
- 14 framework and model governance structure relating to the privacy and
- 15 confidentiality of personal information collected and stored by state executive
- 16 branch agencies, including but not limited to:
- 17 1. Identification of key infrastructure components and how to secure them;
- 18 2. Establishment of a common benchmark that measures the effectiveness
- 19 of security, including continuous monitoring and automation of
- 20 defenses;
- 21 3. Implementation of vulnerability scanning and other security
- 22 assessments;
- 23 4. Provision of training, orientation programs, and other communications
- 24 that increase awareness of the importance of security among agency
- 25 employees responsible for personal information; and
- 26 5. Development of and making available a cyber security incident response
- 27 plan and procedure;~~and~~

- 1 (q) Establishing, publishing, maintaining and implementing comprehensive
2 policy standards and procedures for the responsible, ethical, and
3 transparent use of generative artificial intelligence systems and high-risk
4 artificial intelligence systems, including but not limited to policy standards
5 and procedures that:
6 1. Govern their procurement, implementation, and ongoing assessment;
7 2. Address and provide resources for security of data and privacy; and
8 3. Create guidelines for acceptable use policies for integrating high-risk
9 artificial intelligence systems; and
- 10 (r) Preparing proposed legislation and funding proposals for the General
11 Assembly that will further solidify coordination and expedite implementation
12 of information technology systems.
- 13 (3) The Commonwealth Office of Technology may:
- 14 (a) Provide general consulting services, technical training, and support for
15 generic software applications, upon request from a local government, if the
16 executive director finds that the requested services can be rendered within the
17 established terms of the federally approved cost allocation plan;
- 18 (b) Promulgate administrative regulations in accordance with KRS Chapter 13A
19 necessary for the implementation of KRS 42.720 to 42.742, 45.253, 171.420,
20 186A.040, and 186A.285;
- 21 (c) Solicit, receive, and consider proposals from any state agency, federal agency,
22 local government, university, nonprofit organization, private person, or
23 corporation;
- 24 (d) Solicit and accept money by grant, gift, donation, bequest, legislative
25 appropriation, or other conveyance to be held, used, and applied in accordance
26 with KRS 42.720 to 42.742, 45.253, 171.420, 186A.040, and 186A.285;
- 27 (e) Make and enter into memoranda of agreement and contracts necessary or

- 1 incidental to the performance of duties and execution of its powers, including
2 but not limited to agreements or contracts with the United States, other state
3 agencies, and any governmental subdivision of the Commonwealth;
- 4 (f) Accept grants from the United States government and its agencies and
5 instrumentalities, and from any source, other than any person, firm, or
6 corporation, or any director, officer, or agent thereof that manufactures or
7 sells information resources technology equipment, goods, or services. To
8 these ends, the Commonwealth Office of Technology shall have the power to
9 comply with those conditions and execute those agreements that are
10 necessary, convenient, or desirable; and
- 11 (g) Purchase interest in contractual services, rentals of all types, supplies,
12 materials, equipment, and other services to be used in the research and
13 development of beneficial applications of information resources technologies.
14 Competitive bids may not be required for:
- 15 1. New and emerging technologies as approved by the executive director
16 or her or his designee; or
- 17 2. Related professional, technical, or scientific services, but contracts shall
18 be submitted in accordance with KRS 45A.690 to 45A.725.
- 19 (4) Nothing in this section shall be construed to alter or diminish the provisions of KRS
20 171.410 to 171.740 or the authority conveyed by these statutes to the Archives and
21 Records Commission and the Department for Libraries and Archives.
- 22 (5) The Commonwealth Office of Technology shall, on or before October 1 of each
23 year, submit to the Legislative Research Commission a report in accordance with
24 KRS 57.390 detailing:
- 25 (a) Any security breaches that occurred within organizational units of the
26 executive branch of state government during the prior fiscal year that required
27 notification to the Commonwealth Office of Technology under KRS 61.932;

- 1 (b) Actions taken to resolve the security breach, and to prevent additional security
2 breaches in the future;
- 3 (c) A general description of what actions are taken as a matter of course to protect
4 personal data from security breaches; and
- 5 (d) Any quantifiable financial impact to the agency reporting a security breach.

6 ➔SECTION 3. A NEW SECTION OF KRS 42.720 TO 42.742 IS CREATED TO
7 READ AS FOLLOWS:

8 (1) The Commonwealth Office of Technology shall create an Artificial Intelligence
9 Governance Committee to:

10 (a) Develop policy standards and guiding principles to mitigate risks and
11 protect data and privacy of Kentucky citizens and businesses that adhere to
12 the latest version of Standard ISO/IEC 42001 of the International
13 Organization for Standardization;

14 (b) Establish technology standards to provide protocols and requirements for
15 the use of generative artificial intelligence and high-risk artificial
16 intelligence systems;

17 (c) Ensure transparency in the use of artificial intelligence systems;

18 (d) Maintain a centralized registry to include current inventory of generative
19 artificial intelligence systems and high-risk artificial intelligence systems;
20 and

21 (e) Develop an approval process to include a registry of application, use case,
22 and decision rationale.

23 (2) The Artificial Intelligence Governance Committee shall develop policies and
24 procedures to ensure that any department, program, cabinet, agency, or
25 administrative body that utilizes and accesses the Commonwealth's information
26 technology and technology infrastructure shall:

27 (a) Verify the use and development of generative artificial intelligence systems

- 1 and high-risk artificial intelligence systems, and that any information
2 utilized or produced is trusted, safe, and secure; and
- 3 (b) Act in compliance with responsible, ethical, and transparent procedures to
4 implement the use of artificial intelligence technologies by:
- 5 1. Ensuring artificial intelligence models have comprehensive and
6 complete documentation that is available for review and inspection;
7 2. Requiring validation by humans for bias, unintended consequences,
8 and correctness for all outcomes from generative and high-risk
9 artificial intelligence systems;
10 3. Ensuring the use of generative artificial intelligence and high-risk
11 artificial intelligence systems are resilient, accountable, and
12 explainable; and
13 4. Prohibiting the use of unexplainable artificial intelligence capabilities
14 in any decision-making or approval or denial processes in state
15 government functions.
- 16 (3) The Commonwealth Office of Technology shall prioritize personal privacy and
17 the protection of the data of individuals and businesses as the state develops,
18 implements, employs, and procures artificial intelligence systems, generative
19 artificial intelligence systems, and high-risk artificial intelligence systems by
20 ensuring all departments, agencies, and administrative bodies:
- 21 (a) Allow only the use of necessary data in artificial intelligence systems;
22 (b) Do not allow unrestricted access to personal data controlled by the
23 Commonwealth; and
24 (c) Secure all data and implement a timeframe for data retention.
- 25 (4) To maintain and secure the technology infrastructure, information technology,
26 information resources, and personal information, all departments, agencies, and
27 administrative bodies shall be subject to the centralized approval process in

1 subsection (5) of this section for both the internal and external utilization of
2 generative artificial intelligence systems or high-risk artificial intelligence
3 systems.

4 (5) (a) The Commonwealth Office of Technology shall ensure the implementation
5 of generative artificial intelligence and high-risk artificial intelligence in
6 agency use and business processes is only considered if there is a positive
7 outcome for citizens. A department, agency, or administrative body shall:

8 1. Demonstrate that the use of artificial intelligence is the best solution to
9 yield the intended outcome by examining other technology and process
10 applications available prior to employing the capabilities of artificial
11 intelligence; and

12 2. Provide a statement of intent for each use case of the artificial
13 intelligence application, and indicate whether the outcome of artificial
14 intelligence will make a recommendation to the user or make a
15 determination on behalf of the user.

16 (b) When a department, agency, or administrative body seeks approval to
17 develop, implement, employ, or procure any internal or external artificial
18 intelligence systems, the request shall:

19 1. Be entered into a registry maintained by the Commonwealth Office of
20 Technology; and

21 2. Include the planned artificial intelligence use case and any necessary
22 documentation.

23 (c) The executive director of the Commonwealth Office of Technology shall:

24 1. Review and approve or disapprove each request for use of artificial
25 intelligence; and

26 2. Retain records of the specific artificial intelligence use and decision
27 rationale for an approval or disapproval.

1 (d) At a minimum, the executive director of the Commonwealth Office of
2 Technology shall consider and document:

3 1. Whether the artificial intelligence system is fair and will not result in
4 discrimination against any individual or group of individuals;

5 2. How the use of generative artificial intelligence or other artificial
6 intelligence capabilities will benefit the citizens of the Commonwealth
7 and serve the objectives of the department or agency;

8 3. Whether adequate oversight and human interaction of the artificial
9 intelligence system exists;

10 4. The potential risks, including cybersecurity, data protection and
11 privacy, and health and safety of individuals and businesses, and a
12 mitigation strategy to any identified or potential risk; and

13 5. The proper control and management for all data possessed by the
14 Commonwealth to maintain security and data quality.

15 (6) (a) A department, agency, or administrative body shall disclose to the public,
16 through a clear and conspicuous disclaimer, when generative artificial
17 intelligence, artificial intelligence systems, or other artificial intelligence-
18 related capabilities are used:

19 1. To render any decision regarding individual citizens or businesses
20 within the state;

21 2. In any process, or to produce materials used by the system or humans,
22 to inform a decision or create an output; or

23 3. To produce information or outputs accessible by citizens and
24 businesses.

25 (b) When an artificial intelligence system makes external decisions related to
26 citizens of the Commonwealth, a department, agency, or administrative
27 body shall:

- 1 1. Disclose how artificial intelligence is used in the decision-making
- 2 process;
- 3 2. Provide the extent of human involvement in validating and oversight
- 4 of any decision made; and
- 5 3. Make readily available options for individuals to appeal a
- 6 consequential decision that involves artificial intelligence.
- 7 (c) Any disclaimer under paragraph (a) of this subsection shall also provide
- 8 information regarding third-party artificial intelligence products or
- 9 programs, including but not limited to:
- 10 1. Data sets used;
- 11 2. Data and time parameters in the data set;
- 12 3. Description of biases embedded in the program; and
- 13 4. Any warranties provided by the owner of the artificial intelligence
- 14 program and subsequent data outputs.
- 15 (7) All departments, agencies, and administrative bodies shall submit for review all
- 16 third-party high-risk artificial intelligence developers, system administrators,
- 17 providers, and contractors by the Commonwealth Office of Technology in order
- 18 to mitigate the risk of data breaches, unauthorized access, or misuse of personal
- 19 information. The review process shall include but is not limited to:
- 20 (a) Assessing the ability to deliver value to the citizens of the Commonwealth
- 21 and evaluate their trust, safety, and security procedures;
- 22 (b) Ensuring utilization of the Commonwealth's data collection and utilization
- 23 standards, comply with any applicable laws, policies, and administrative
- 24 regulations, and adhere to the latest version of Standard ISO/IEC 42001 of
- 25 the International Organization for Standardization;
- 26 (c) Reviewing the results of testing conducted by the developer to verify the
- 27 efficacy of the generative artificial intelligence or high-risk artificial

1 intelligence systems, including but not limited to:

2 1. The cybersecurity and physical security;

3 2. The potential risks associated; and

4 3. Any of the potential biases that could result in unlawful
5 discrimination;

6 (d) Assessing the audit reports, product roadmaps, warranties, terms of service,
7 end-user license agreements, contracts, and any other documentation in the
8 assessment of risk management activities; and

9 (e) Implementing and maintaining a comprehensive inventory of all third-party
10 material used or required for the use of all third-party generative artificial
11 intelligence or other artificial intelligence related capabilities;

12 (8) The Commonwealth Office of Technology shall establish policies to encompass
13 legal and ethical frameworks to ensure that any artificial intelligence systems
14 shall align with existing laws, administrative regulations, and guidelines, which
15 shall be updated at least annually to maintain compliance as technology and
16 industry best practices evolve.

17 (9) Operating standards for utilization of high-risk artificial intelligence systems
18 shall:

19 (a) Prohibit the use of a high-risk artificial intelligence system to render a
20 consequential decision without the design and implementation of a risk
21 management policy and program for high-risk artificial intelligence
22 systems. The risk management policy shall;

23 1. Specify principles, process, and personnel that shall be utilized to
24 maintain the risk management program; and

25 2. Identify, mitigate, and document any bias or potential bias that is a
26 potential consequence of use in making a consequential decision; and

27 (b) Each risk management policy designed and implemented shall at a

1 minimum adhere to the latest version of Standard ISO/IEC 42001 of the
2 International Organization for Standardization, or another national or
3 internationally recognized risk management framework for artificial
4 intelligence systems, and consider:

5 1. The size and complexity of the deployer;

6 2. Nature and scope and intended use of the high-risk artificial
7 intelligence system and its deployer; and

8 3. The sensitivity and volume of data processed.

9 (10) (a) The use of a high-risk artificial intelligence system shall not be used to
10 make a consequential decision without a completed impact assessment that
11 shall be completed before initial use and no later than ninety (90) days after
12 each significant update.

13 (b) Each impact assessment for a high-risk artificial intelligence system shall
14 include but not be limited to:

15 1. A statement disclosing the purpose, intended use case, and benefits;

16 2. Identify if the use creates a potential risk and measures to prevent bias
17 or unlawful discrimination;

18 3. A statement that any post-deployment assessments for significant
19 updates are consistent with or vary from the agency's intended use;

20 4. A description of categories of the process inputs and outputs,
21 including any description of data categories used for customization;

22 5. A list of any metrics for performance evaluation and known
23 limitations;

24 6. A description of transparency measures; and

25 7. A description of monitoring, user safeguards, and any oversight
26 processes to address issues from the implementation or use of a
27 high-risk artificial intelligence system.

1 (11) The Commonwealth Office of Technology shall provide education and training of
2 employees about the benefits and risks of artificial intelligence and allowable use
3 policies.

4 (12) (a) The Commonwealth Office of Technology shall transmit reports to the
5 Legislative Research Committee and the Interim Joint Committee on State
6 Government by December 1, 2025, and annually every year thereafter. The
7 reports shall include:

8 1. The artificial intelligence registry in subsection (5)(b)1. of this section,
9 which shall include the current inventory of artificial intelligence
10 utilized in state government;

11 2. Applications received for use of artificial intelligence, including the
12 decision and rationale in approving or disapproving a request in
13 compliance with subsection (5)(c) of this section; and

14 3. Third-party artificial intelligence developers, system administrators,
15 providers, and contractors submitted for review in compliance with
16 subsection (5) of this section.

17 (b) To facilitate the report in paragraph (a) of this subsection the
18 Commonwealth Office of Technology shall receive from each department,
19 agency, and administrative body a report examining and identifying
20 potential use cases for the deployment of generative artificial intelligence
21 systems and high-risk artificial intelligence systems, including a description
22 of the benefits and risks to individuals, communities, government and
23 government, employees.

24 (13) The Commonwealth Office of Technology shall promulgate administrative
25 regulations in accordance with KRS Chapter 13A to implement this section and
26 Section 2 of this Act by July 1, 2025.

27 ➔Section 4. KRS 117.001 is amended to read as follows:

1 As used in this chapter~~[, unless the context otherwise requires]~~:

- 2 (1) "Audit log" means a detailed record of all actions and events that have occurred on
3 the voting system, including:
- 4 (a) Log-in attempts with username and time stamp;
 - 5 (b) Election definition and setup;
 - 6 (c) Ballot preparation and results processing;
 - 7 (d) Diagnostics of any type; and
 - 8 (e) Error and warning messages and operator response;
- 9 (2) "Automatic tabulating equipment" means apparatus necessary to automatically
10 examine and count votes as designated on ballots and data processing machines
11 which can be used for counting ballots and tabulating results;
- 12 (3) "Ballot" or "official ballot" means the official presentation of offices and candidates
13 to be voted for, including write-in candidates, and all public questions submitted for
14 determination, and shall include a voting machine ballot, a paper ballot, an absentee
15 ballot, a federal provisional ballot, a federal provisional absentee ballot, or a
16 supplemental paper ballot which has been authorized for the use of voters in any
17 primary, regular election, or special election by the Secretary of State or the county
18 clerk;
- 19 (4) "Ballot box" means any box, bag, or other container that can be locked, sealed, or
20 otherwise rendered tamper-resistant, for receiving ballots;
- 21 (5) "Ballot marking device" means any approved device for marking a ballot which
22 will enable the ballot to be tabulated manually or by means of automatic tabulating
23 equipment;
- 24 (6) "Election" or "elections" means any primary, regular election, or special election;
- 25 (7) "Election officer" has the same meaning as in KRS 118.015;
- 26 (8) (a) "Electioneering communication" means any communication broadcast by
27 cable, internet, television, or radio, printed in a newspaper or on a billboard,

1 directly mailed or delivered by hand to personal residences, or in telephone
2 calls made to personal residences, otherwise distributed that:

- 3 1. Unambiguously refers to any candidate for any state, county, city, or
4 district office, or to any ballot measure;
5 2. Occurs within forty-five (45) days before a primary or general
6 election; and
7 3. Is received by an audience that includes members of the electorate for
8 such public office or the electorate associated with the ballot
9 containing the ballot measure.

10 (b) "Electioneering communication" does not include:

- 11 1. Any news articles, editorial endorsements, opinions or commentary,
12 writings, or letters to the editor printed in a newspaper, magazine, or
13 other periodical not owned or controlled by a candidate, committee, or
14 political party;
15 2. Any editorial endorsements or opinions aired by a broadcast facility
16 not owned or controlled by a candidate, committee, or political party;
17 3. Any communication by persons made in the regular course and scope
18 of their business or any communication made by a membership
19 organization solely to members of such an organization and their
20 families;
21 4. Any communication that refers to any candidate only as part of the
22 popular name of a bill or statute; or
23 5. A communication that constitutes a contribution or independent
24 expenditure as defined in KRS 121.015;

25 (9) "E-poll book" means an electronic device capable of holding a file of voter data and
26 related information for use in identifying registered voters prior to a voter's
27 receiving or casting a ballot, and allowing a voter to electronically sign in on an

1 electronic registered voter roster in lieu of signing a paper registered voter roster;

2 ~~(10)~~~~(9)~~ "Federal provisional voter" means a person:

3 (a) Who does not appear to be registered to vote;

4 (b) Whose name does not appear on the precinct roster;

5 (c) Who has not provided proof of identification to the precinct election officer
6 before voting in a federal election; and

7 (d) Who elects to proceed with voting a federal provisional ballot under KRS
8 117.229;

9 ~~(11)~~~~(10)~~ "Federal provisional ballot" or "federal provisional absentee ballot" means
10 ballots which have been authorized by the Secretary of State or the county clerk to
11 be used by federal provisional voters in any federal primary or election;

12 ~~(12)~~~~(11)~~ "Information content provider" means any person or entity that is
13 responsible, in whole or in part, for the creation or development of information
14 provided through the internet or any other interactive computer service;

15 ~~(13)~~ "Inner envelope" or "secrecy envelope" means the envelope provided to the voter
16 with a ballot into which the voter shall place his or her voted ballot;

17 ~~(14)~~ "Interactive computer service" means any information service, system, or access
18 software provider that provides or enables computer access by multiple users to a
19 computer server, including specifically a service or system that provides access to
20 the internet and such services offered or systems operated by libraries or
21 educational institutions;

22 ~~(15)~~~~(12)~~ "Political group" has the same meaning as in KRS 118.015;

23 ~~(16)~~~~(13)~~ "Political organization" has the same meaning as in KRS 118.015;

24 ~~(17)~~~~(14)~~ "Precinct ballot counter" means an automatic tabulating device used at the
25 precinct to tabulate and process ballots;

26 ~~(18)~~~~(15)~~ "Proof of identification" means a document that was issued by:

27 (a) The United States or the Commonwealth of Kentucky, and the document

1 contains:

2 1. The name of the individual to whom the document was issued; and

3 2. A photograph of the individual to whom the document was issued;

4 (b) The United States Department of Defense, a branch of the uniformed services,
5 the Merchant Marine, or the Kentucky National Guard, and the document
6 contains:

7 1. The name of the individual to whom the document was issued; and

8 2. A photograph of the individual to whom the document was issued;

9 (c) A public or private college, university, or postgraduate technical or
10 professional school located within the United States, and the document
11 contains:

12 1. The name of the individual to whom the document was issued; and

13 2. A photograph of the individual to whom the document was issued; or

14 (d) Any city government, county government, urban-county government, charter
15 county government, consolidated local government, or unified local
16 government, which is located within this state, and the document contains:

17 1. The name of the individual to whom the document was issued; and

18 2. A photograph of the individual to whom the document was issued;

19 (19) "Sponsor" means the person or entity paying for the electioneering
20 communication. If a person or entity acts as an agent for another or is
21 reimbursed by another for the payment, the original source of the payment is the
22 sponsor;

23 (20) (a) 1. "Synthetic media" means an image, audio recording, or video
24 recording of an identifiable natural individual's appearance, action,
25 or speech that has been intentionally manipulated with the use of
26 generative adversarial network techniques or other digital technology
27 in a manner to create a realistic but false image, audio, or video that

1 produces:

2 a. A depiction that, to a reasonable individual, is of an identifiable
3 natural individual in appearance, action, or speech that did not
4 actually occur in reality and that was created without the consent
5 of such individual; and

6 b. A fundamentally different understanding or impression of the
7 appearance, action, or speech than a reasonable person would
8 have from the unaltered, original version of the image, audio
9 recording, or video recording.

10 2. As used in this subparagraph:

11 a. "Generative adversarial network" means a machine learning
12 model that uses neural networks to develop new data and make
13 more accurate predictions; and

14 b. "Neural network" means a machine learning algorithm modeled
15 on the human brain and nervous system.

16 (b) "Synthetic media" does not include content that contains a disclosure
17 under subsection (2) of Section 5 of this Act.

18 (21)[(16)] "Voting booth" or "ballot completion area" means an area in which a voter
19 casts his or her vote or completes his or her ballot which is designed to ensure the
20 secrecy of the vote;

21 (22)[(17)] "Vote center" means a consolidated precinct of the county;

22 (23)[(18)] "Voting equipment" means any physical component of a voting system and
23 includes voting machines where voting machines are in operation;

24 (24)[(19)] "Voting machine" or "machine":

25 (a) Means a part of a voting system that consists of one (1) or more electronic
26 devices that operate independently or as a combination of a ballot marking
27 device and an electronic or automatic vote tabulation device; and

1 (b) Does not include an e-poll book;

2 ~~(25)~~~~(20)~~ "Voting system":

3 (a) Means the total combination of physical, mechanical, electromechanical, or
4 electronic equipment, including the software, hardware, firmware, and
5 documentation required to program, control, and support that equipment, that
6 is used to:

- 7 1. Define ballots;
8 2. Cast and count votes;
9 3. Report or display election results; and
10 4. Maintain and produce any audit trail information;

11 (b) Includes the practices and associated documentation used to:

- 12 1. Identify system components and versions of those components;
13 2. Test the system during its development and maintenance;
14 3. Maintain records of system errors and defects;
15 4. Determine specific system changes to be made to a system after the
16 initial qualification of the system;
17 5. Make available any materials to the voter, such as notices, instructions,
18 forms, or paper ballots; and

19 (c) Does not include an e-poll book; and

20 ~~(26)~~~~(21)~~ "Voter-verified paper audit trail" means a contemporaneous paper record of a
21 ballot printed for the voter to confirm his or her votes before the voter casts his or
22 her ballot that:

- 23 (a) Allows the voter to verify the voter's ballot choices before the casting of the
24 voter's ballot;
25 (b) Is not retained by the voter;
26 (c) Does not contain individual voter information;
27 (d) Is produced on paper that is sturdy, clean, and resistant to degradation; and

- (e) Is readable in a manner that makes the voter's ballot choices obvious to the voter or any person without the use of computer or electronic code.

➔SECTION 5. A NEW SECTION OF KRS CHAPTER 117 IS CREATED TO READ AS FOLLOWS:

(1) Any election officer or candidate for any elected office whose appearance, action, or speech is altered through the use of synthetic media in an electioneering communication may:

(a) Seek injunctive or other equitable relief against the sponsor of the electioneering communication prohibiting the publication of that synthetic media; and

(b) Bring an action for damages against the sponsor of the electioneering communication. The court may also award a prevailing party reasonable attorney's fees and costs. This paragraph does not limit or preclude a plaintiff from securing or recovering any other available remedy.

(2) It is an affirmative defense for any action brought under subsection (1) of this section that the electioneering communication containing synthetic media includes a disclosure that is clear and conspicuous and included in, or alongside and associated with, the content in a manner that is likely to be noticed by the user.

(3) Any action brought under subsection (1) of this section shall be filed in the Circuit Court of the county in which the plaintiff resides.

(4) In any action brought under subsection (1) of this section, the plaintiff bears the burden of establishing the use of synthetic media by clear and convincing evidence.

(5) In any action brought under subsection (1) of this section:

(a) The sponsor of the electioneering communication may be held liable; and

(b) The medium disseminating the electioneering communication and the

1 advertising sales representative of such medium shall not be held liable,
2 except as provided in subsection (6) of this section.

3 (6) Except when a licensee, programmer, or operator of a federally licensed
4 broadcasting station transmits an electioneering communication that is subject to
5 47 U.S.C. sec. 315, a medium or its advertising sales representative may be held
6 liable in a cause of action brought under subsection (1) of this section if:

7 (a) The person intentionally removes any disclosure described in subsection (2)
8 of this section from the electioneering communication it disseminates and
9 does not remove the electioneering communication or replace the disclosure
10 when notified; or

11 (b) Subject to affirmative defenses described in subsection (2) of this section,
12 the person changes the content of an electioneering communication in a
13 manner that results in it qualifying as synthetic media.

14 (7) (a) A provider or user of an interactive computer service shall not be treated as
15 the publisher or speaker of any information provided by another
16 information content provider.

17 (b) An interactive computer service may be held liable in accordance with
18 subsection (6) of this section.

19 (8) Courts are encouraged to determine matters under this section expeditiously.

20 ➔Section 6. Whereas implementing governance to maximize the opportunities for
21 the responsible and ethical use of artificial intelligence is vitally important to combat the
22 critical impact artificial intelligence can have on the security of data and information in
23 the Commonwealth and it is critically important to protect candidates and election
24 officers from fraudulent misrepresentations of themselves and their issues, an emergency
25 is declared to exist, and this Act takes effect upon its passage and approval by the
26 Governor or upon its otherwise becoming a law.