JCOTS

JOINT COMMISSION ON TECHNOLOGY & SCIENCE

Bill Study

Government Organizational Structure: Office of the Attorney General

November 2025

Executive Summary

The rapid pace of technological innovation—from artificial intelligence and blockchain to data privacy and digital consumer protection—will continue to create new and complex legal challenges for state governments. This paper examines the capacity of the Virginia Office of the Attorney General (OAG) to effectively enforce laws related to emerging technologies. It evaluates the OAG's current key priorities, organizational structure, and technical expertise to determine its readiness to address evolving issues.

The study finds that the OAG is well positioned to become a leader in technology enforcement if it proactively modernizes its capabilities. Strengthening internal capacity by establishing a dedicated technology enforcement unit will be a critical step toward ensuring that the Commonwealth can protect consumers and promote responsible innovation.

Current Key Priorities

The Virginia Office of the Attorney General is responsible for a wide range of enforcement actions across the Commonwealth. Its top priorities are reducing violent crime across the Commonwealth, combating the opioid crisis, and protecting Virginia's senior citizens. Through Operation Ceasefire, the OAG has worked with law enforcement partners in targeting communities to reduce violent crimes. In addressing the opioid crisis, the OAG has focused on holding pharmaceutical companies accountable and settlements from these cases have directed funds to the Opioid Abatement Authority, where they are used to support treatment and recovery efforts across Virginia. In an effort to protect seniors, the TRIAD program works in partnership with local law enforcement and social services agencies to raise awareness about scams and frauds targeting seniors, with active chapters across the Commonwealth.

Although technology is not currently noted as a key priority, the OAG is concerned about technological crimes especially involving vulnerable populations such as children and anticipate the need to focus more on the area of emerging technologies in the coming years.

Technology Enforcement

Current Challenges

In addition to the absence of dedicated staff to educate and prevent issues surrounding emerging technologies, the OAG indicated that they currently face several notable challenges in enforcing laws

that deal with technology. One of the most significant is what they describe as a broad immunity granted to online platforms under Section 230 of the Communications Decency Act. This federal law can shield technology companies from liability when a claim would treat them as a publisher of third-party content. The OAG has found courts frequently dismiss cases on Section 230 grounds at early stages of litigation, which can prevent meaningful enforcement and reduce accountability among technology companies.

Another difficulty arises from the use of forum selection clauses in the terms and conditionals of major technology companies, which often require disputes to be brought in jurisdictions like California. In some cases, private litigation involving similar issues is consolidated into multidistrict litigation, which can further complicate Virginia's ability to pursue cases in preferred forums. Additionally, coordinating with other states on multi-state investigations and enforcement can present complexities, as each state has its own legal frameworks and requirements that can slow or complicate joint efforts.

Future Challenges

The OAG anticipates that the rapidly evolving nature of technology will continue to pose challenges, particularly as legal frameworks lag behind technological advancements. For example, new technologies such as artificial intelligence present emerging privacy concerns that will require resource-intensive, ongoing legislative evaluation and adaptation of enforcement strategies. Additionally, the OAG strives to play a role in prevention which also presents challenges in a constantly evolving environment.

The OAG indicated that certain statutory requirements, such as the cure provision in the Virginia Consumer Data Protection Act, can limit enforcement options. Under this provision (59.1-584 B), suspected violators must be given the opportunity to cure a violation within a 30-day window before a lawsuit can be filed, and if the violation is cured, no suit may proceed. This limits the ability to publicly disclose outcomes or hold violators accountable through litigation.

Finally, the increasing complexity of technology and data privacy issues will continue to place demands on the resources and technical expertise necessary for effective enforcement. The crossover of technological development and law enforcement creates challenges for department specialization. The need for vocational crossover between technology and law is apparent as technological developments continue, yet attorneys with technical experience are limited.

Organizational Structure

The Virginia Office of the Attorney General has approximately 585 full-time staff and is comprised of five primary legal divisions:

1. Criminal Justice and Public Safety
2. Government Operations and Transactions
3. Civil Litigation
4. Health, Education, and Social Services
5. Solicitor General's Office

In total, across these legal divisions, there are 27 sections. In addition to the legal divisions, the OAG has a Program and Outreach Division composed of non-attorney staff who manage various public-facing initiatives.

Sections the OAG range in size but typically include one or more of the following positions:

- Senior Assistant Attorney General
- Assistant Attorney General III
- Assistant Attorney General II
- Assistant Attorney General I
- Paralegal II
- Investigator
- Dispute Resolution
- Legal Secretary

Technology Capacity

Of the 27 sections, within the OAG several have responsibilities that intersect, but are not tasked exclusively with, technology.

1. Criminal Justice and Public Safety include:
   - Computer Crimes Section (3 Attorneys, 3 Staff)

   Address cases that involve emerging technological threats as part of its broader portfolio.

2. Government Operations and Transactions include:
   - Technology and Procurement (6 Attorneys)

   Provides counsel on technology procurement matters for client agencies.

3. Civil Litigation includes:
    - Consumer Protection
        - Consumer Privacy (2 Attorneys, 2 Staff)

Enforces consumer protection laws as they are related to technology, particularly in addressing issues involving large technology companies.

The Consumer Privacy Unit was established following the enactment of the Virginia Consumer Data Protection Act (CDPA). This unit investigates and prosecutes violations of state and federal privacy laws including the CDPA, the Virginia Genetic Data Privacy Act, and the federal Children's Online Privacy Protection Act.

State Focus: Colorado

Background
The Colorado OAG has approximately 750 employees and data privacy and cybersecurity have historically been handled within the Consumer Fraud Unit of the Consumer Protection Section. There is a full-time cybersecurity fellow responsible for all data breach intake and attorneys in Consumer Fraud would support that fellow as the cases evolved.

In 2022 the Colorado Privacy Act passed and funding was allocated for two attorneys to handle the rulemaking. When the rulemaking was done and the Privacy Act went into effect in July 2023, those positions shifted to enforcement. During that time, it became clear their expertise would be helpful in other areas that dealt with technology.

Technology and Privacy Protection Unit
In January 2025 the OAG established the Technology and Privacy Protection Unit within the Consumer Protection Section. Consumer Protection is the largest office within the Colorado OAG with 120 employees. The Technology and Privacy Protection Unit is comprised of three attorneys, a cybersecurity fellow, and one technologist. One of the attorney's is a lead or "first" attorney who reports to a Deputy of Consumer Protection. That position manages the unit and maintains 1-2 cases. As of July 2025, they are actively recruiting for the Technologist position and see this as a critical role in providing technical expertise for theirs and other units within Consumer Protection.

The overall responsibilities of the Technology and Privacy Protection Unit include rulemaking, bill review, and enforcement. Enforcement extends across many areas including the Colorado Privacy Act, Colorado AI Act (effective 2/26), all cybersecurity and data breach notification laws, and other technology focused laws including any of the specialized technology bills that fall under the Unfair and Deceptive Acts and Practices (UDAP) statute. They also handle the application of the Colorado Consumer Protection Act as it applies to emerging technologies.

The Technology and Privacy Protection Unit may take the lead in some cases but are primarily a resource for the broader Consumer Protection group as technology becomes more a part of what they do. Both Technology and Privacy Protection or attorneys from Consumer Fraud will lead, depending on availability. Since their role is consultative in nature, cross training is key. Colorado has an additional Technology Unit, outside of Consumer Protection, that advises the state agencies on how they should be in compliance with privacy, cyber security, and AI Laws.

Policy Recommendations

JCOTS recommends considering the establishment of a dedicated Technology unit, within the OAG's Division of Civil Litigation, that would be responsible for the oversight and enforcement of laws pertaining to cybersecurity, data privacy, artificial intelligence (AI), algorithmic pricing, and other emerging technologies. To be most effective, the attorneys should have a background practicing in technology. Staffing levels should be consistent with other sections of the OAG which include attorneys, a paralegal, investigators, a legal secretary, and a dispute resolution role (Appendix I).

In addition, JCOTS recommends adding the role of Technologist (non-attorney) to advise on technical issues related to digital privacy, cybersecurity, artificial intelligence, machine learning, human-computer interaction and other topics that may arise. According to the Colorado OAG, Oregon, Massachusetts, and Delaware have hired a Technologist within their Consumer Protection or Privacy Units. The role of a Technologist also exists in the Federal Government within the Federal Trade Commission, the Federal Communications Commission, and the Consumer Product Safety Commission. The job posting from Colorado's active recruitment may be used as a model (Appendix II).

The OAG anticipates that the rapidly evolving nature of technology will continue to pose challenges, particularly as legal frameworks lag behind technological advancements. Considering this, the OAG is supportive of the idea of expansion of their workforce to cover legal responsibilities that should, and are likely to, arise with the emergence of new technologies.

Additional Responsibilities

The establishment of a Technology Unit will provide the OAG with the ability to expand its reach beyond enforcement. The OAG can play a critical role in shaping the legal and policy landscape surrounding emerging technologies through its advisory and educational functions.

As a chief legal advisor to the Governor, the General Assembly, and state agencies, the OAG provides guidance on the implications of technologies including reviewing legislation to ensure that new technology laws are enforceable, balanced, and adaptable to innovation. Beyond legal counsel, the Attorney General's Office can also serve as a key public educator, issuing consumer advisories about technology-related risks like online scams, data breaches, and AI-enabled fraud. It can offer compliance guidance to businesses developing or deploying emerging technologies, helping to promote lawful innovation while protecting the public. Through these responsibilities, the OAG can ensure that the Commonwealth's approach to technology remains both forward-looking and accountable.

Appendix I

Positions in the proposed Technology Unit.

Position Title	Salary	Benefits (approx. 33%)	QTY	Total (USD)
Senior Assistant Attorney General	119,438	39,415	1	158,853
Assistant Attorney General III	106,838	35,257	2	284,189
Assistant Attorney General II	94,238	31,099	1	125,337
Assistant Attorney General I	83,213	27,460	1	110,673
Paralegal-III	64,954	21,435	1	86,389
Investigators	75,000	24,750	2	199,500
Dispute Resolution	51,578	17,021	1	68,599
Legal Secretary	50,857	16,783	1	67,640
Technologist	110,000	36,300	1	146,300
				1,247,479

Appendix: II

Job Posting for the position of Technologist within the Colorado Office of the Attorney General.

The Consumer Protection Section is seeking a talented, enthusiastic, and experienced person to join its team as a technologist. Technologists are technology and digital market subject matter experts who will work alongside attorneys and staff to protect Colorado consumers. This position will involve investigating, understanding and explaining technologically complex issues relating to investigations and initiatives pursued by Consumer Protection attorneys, including attorneys in the Technology & Privacy Protection Unit, Consumer Credit Unit, and Antitrust Unit. While the Technologist will not be expected to be an expert in all areas, they will be expected to learn and explain the technological intricacies of digital privacy, online data flows, online advertising, cybersecurity, artificial intelligence, machine learning, algorithmic design, application development, and human-computer interaction. If you're interested in putting your technology expertise to work in a public service environment, this may be the opportunity you've been looking for!

WHAT YOU WILL DO

In this role as Technologist (Information Technology V) you will apply your technical expertise to assist in cybersecurity, data privacy, consumer fraud, and other consumer protection investigations into unfair and deceptive business practices and underlying technologies. You will be a core team member focused on identifying and responding to current and next-generation threats. This work will span a wide range of technical matters and related policy issues in the Consumer Protection Section and Department of Law as well as working with other state agencies. The Technologist will research, evaluate, and report on new and emerging technical developments relevant to the Consumer Protection units and work with legal experts on investigatory opportunities, mitigation strategies, and possible remedies. The Technologist will generally be expected to:

- Identify and explain complex technological elements of unfair business practices and strengthen investigations into those practices by helping to in craft targeted civil investigative demands;
- Aid in the review and analysis of data and documents related to investigations and investigative findings;
- Conduct presentations and briefings of investigative conclusions through written reports;
- Support the development of case theories and aid in the creation of effective remedies;
- Serve as an expert advisor to enforcement staff regarding technology and privacy;
- Deploy or design research methods, validation procedures, and execution plans to evaluate functionality of data privacy and data security technologies; and
- Develop technology-related policies, procedures, tools, examination techniques, and inquiry methods to be applied in connection with consumer protection.

In addition to supporting Consumer Protection section investigations, the Technologist may also provide strategic guidance on technology matters through report recommendations and participate in legislative and policy recommendations.

Experience working in a legal setting or on government or internal investigations may be helpful, but is not required. What is important to us is experience in, and enthusiasm for, technology, problem solving, and working in the public interest. We are looking for people who enjoy being part of a fun, cohesive, and dedicated team that cares deeply about their service to the State of Colorado. People in this unit are successful because they both enjoy their autonomy and thrive in a collaborative environment where people work together to help each other succeed.

WHAT WE ARE LOOKING FOR

Minimum Qualifications and Substitutions: Please document all relevant experience in detail on your application. Experience will not be inferred or assumed. Any part-time experience listed will be prorated.

Experience Only:

Requires eight (8) years of experience in advanced technology research, technology policy, software engineering, or information technology security, two of which must be as an expert advisor, supervisor, or work leader.

OR

Education and Experience:

Requires a bachelor's degree in a quantitative field or equivalent experience in computer science, quantitative analysis, data science, or a related field AND four years of experience in advanced technology research, technology policy, software engineering, or information technology security, two of which must be as an expert advisor, supervisor, or work leader.

Preferred Qualifications: In addition to the minimum qualifications, the preferred applicant will also demonstrate and clearly describe the following skills and experience in their job application:

- Experience using data, research, data science, or user needs to spot issues and develop solutions to novel problems.
- A graduate degree in a quantitative field or comparable experience.
- An understanding of or interest in data privacy, data security, the internet and digital markets, algorithmic discrimination, machine learning, with demonstrated expertise in at least one of these areas and willingness to gain expertise in others.
- Good problem-solving skills and the confidence to know when to ask questions.
- Interest in and/or commitment to public service and diversity, equity, and inclusion efforts.
- Strong organizational and analytical skills with the ability to multi-task.
- Three or more years of specialized technical expertise in technology research, technology policy, software engineering, or security.
- Experience conducting research, auditing, testing, or forensics on systems that impact consumers and consumer privacy.
- Experience testing or implementing systems that effectuate consumer privacy choices.
- Demonstrated ability to simplify complex technical subjects and communicate them to a lay audience. Experience advising and communicating with senior leaders and stakeholders on technical concepts.
- Excellent written and verbal communication skills.
- Working knowledge of computer programming and data analysis. Experience with technical aspects of data security, app development, and networking are preferred.
- Comfort using a range of technical approaches or human-centered design methods involving quantitative and qualitative data collection efforts.
- Experience in the consulting or legal support fields, ideally related to consumer privacy and other related technology.
- Expertise examining large data sets using scripting languages and computational languages (e.g., Python, R, SQL, etc.) to investigate allegations of illegal conduct.
- Experience analyzing, collecting, and using information and data for law enforcement or investigation purposes.
- Ability to be self-directed and manage one's own workload.

Author Information

Jodi Kuhn
Executive Director, Joint Commission on Technology & Science

Contact: info@jcots.virginia.gov

Thanks To

Virginia Office of the Attorney General
Colorado Office of the Attorney General
For providing helpful information and background during the preparation of this report