**Testimony in Support of HB 425 (2021)**

*Criminal Law – Crimes Involving Computers*

Judiciary Committee, February 2, 2021

Sponsor: Delegate Barron

Testimony by: Markus Rauschecker, JD, Cybersecurity Program Director, University of Maryland Center for Health & Homeland Security (CHHS) and Adjunct Faculty at University of Maryland Francis King Carey School of Law

I offer this testimony in support of HB 425 in my personal capacity.

Ransomware is a serious and growing threat

Cybercrime is escalating at an unfathomable pace and is costing victims billions of dollars. One of the most concerning areas of cybercrime is ransomware, whereby cyber criminals prevent a victim from accessing their own computer files through encryption until the victim pays a ransom. Losses from ransomware have increased significantly.[1]

Hospitals, school districts, state and local governments, law enforcement agencies, large and small businesses, and individuals have all been targeted by ransomware attacks. The consequences of these types of attacks can be catastrophic. The inability to access important data could mean the cessation of vital services, financial losses, and even death in cases where electronic patient records are encrypted.

Given the serious potential consequences of ransomware attacks, more must be done to deter cyber criminals from launching such attacks.

HB 425 establishes necessary and strong deterrents against the use of ransomware

By explicitly outlawing the possession of ransomware with the intent to use it, HB 425 establishes a strong deterrent against this type of malicious software. HB 425 makes it very clear to cybercriminals that the mere possession of ransomware with the intent to use it is a crime. Cybercriminals have to be wary of prosecution from the moment they come into possession of the ransomware malware.

Moreover, HB 425 establishes significant penalties for the possession of ransomware which is a strong and effective step towards deterrence.

[1]Ransomware Attacks Grow, Crippling Cities and Businesses
https://www.nytimes.com/2020/02/09/technology/ransomware-attacks.html .

Explicitly criminalizing the possession of ransomware software provides significant advantages over the current extortion statute

HB425 takes a preventive approach to combat ransomware that offers some distinct advantages over the subsumption or inclusion of ransomware attacks as a form of extortion.

By criminalizing the possession of ransomware without research purposes, HB 425 empowers local law enforcement and prosecutors to investigate and prosecute attackers before they act, potentially reducing the risk of harm to public and private cyber-infrastructure.

The specific sanction for ransomware possession also gives prosecutors a wider range of options in cases when the evidence for extortion charges may be difficult to prove. HB 425 shifts the focus of prosecution to mere possession of ransomware malware. As such, the search for evidence will be localized to the computer system of the suspect and there is no longer a need to trace a ransomware attack back to a source nor prove the resulting harm of the attack.

Providing a civil cause of action to victims of ransomware will result in a greater likelihood of recovery for victims

Given the magnitude of cybercrime, government simply does not have the capacity to prosecute every instance of ransomware.[2] Prosecutors have to make strategic and practical decisions about what cases they pursue. It is inevitable that some instances of ransomware will therefore not be prosecuted. If no right to civil action is provided to victims, the victims of ransomware may be left without recourse when government is unable to prosecute. HB 425 addresses this problem by establishing a civil right of action for victims through which they may be able to recover damages.

HB 425 follows other states that have passed legislation which explicitly addresses ransomware

HB 425 follows legislation that has passed in other states which explicitly address ransomware. California, Connecticut, Michigan, Texas, West Virginia, and Wyoming have all passed laws on ransomware.[3] The threat and cost of ransomware are giving rise to a trend of states passing legislation on this issue.

For all of the foregoing reasons, I strongly support HB 425.

---

[2] See Police Executive Research Forum, The Role of Local Law Enforcement Agencies in Preventing and Investigating Cybercrime, available at: http://www.policeforum.org/assets/docs/Critical_Issues_Series_2/the%20role%20of%20local%20law%20enforcement%20agencies%20in%20preventing%20and%20investigating%20cybercrime%202014.pdf

[3] See National Conference of State Legislatures , available at: http://www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws.aspx