**2021-02-25 SB 623 (Support).pdf**
Uploaded by: Jung, Roy
Position: FAV

**BRIAN E. FROSH**
*Attorney General*

**ELIZABETH F. HARRIS**
*Chief Deputy Attorney General*

**CAROLYN QUATTROCKI**
*Deputy Attorney General*

**STATE OF MARYLAND**
**OFFICE OF THE ATTORNEY GENERAL**

FACSIMILE NO.

WRITER'S DIRECT DIAL NO.
410-576-6584

February 25, 2021

TO: The Honorable William C. Smith, Jr.
Chair, Judicial Proceedings Committee

FROM: The Office of the Attorney General

RE: SB 623 – Criminal Law - Crimes Involving Computers – **Letter of Support**

---

The Office of the Attorney General urges the Judicial Proceedings Committee to favorably report SB 623. Senator Lee's SB 623 prohibits acts that interrupt or impair the function of a health care facility, or a public school. The legislation also prohibits the intentional use of ransomware and allows a civil claim for damages caused by prohibited actions.

The incidence of cybersecurity attacks has been increasing steadily over time. In 2019, 205,280 organizations were hacked in ransomware attacks and this is a 41 percent increase compared to 2018.[1] According to the F.B.I., these attacks are becoming "more targeted, sophisticated, and costly" and ransomware, especially, is "the most serious cybercriminal problem[] we face right now."[2] The legislation codifies this concern to deter cyber-attacks through imposing punishments and allows victims to recover damages. It is critical for our State to have laws to fight against cybercrimes, and SB 623 is yet another means to do so.

For the foregoing reasons, the Office of Attorney General urges a favorable report on SB 623.

cc: Senator Lee & Members of the Judicial Proceedings Committee

[1] Nathaniel Popper, *Ransomware Attacks Grow, Crippling Cities and Businesses*, N.Y. TIMES (Feb. 9, 2020), https://www.nytimes.com/2020/02/09/technology/ransomware-attacks.html#:~:text=In%202019%2C%20205%2C280%20organizations%20submitted,helps%20companies%20hit%20by%20ransomware.
[2] *Id.* (internal quotations omitted).

**SB623_FAV_Lee_2021_ml.pdf**
Uploaded by: Lee, Susan
Position: FAV

SUSAN C. LEE
*Legislative District 16*
Montgomery County

MAJORITY WHIP

Judicial Proceedings Committee

Joint Committee on
Cybersecurity, Information Technology,
and Biotechnology

*Chair Emeritus*
Maryland Legislative Asian American
and Pacific Islander Caucus

*President Emeritus*
Women Legislators of the
Maryland General Assembly, Inc.

THE SENATE OF MARYLAND
ANNAPOLIS, MARYLAND 21401

James Senate Office Building
11 Bladen Street, Room 223
Annapolis, Maryland 21401
410-841-3124 · 301-858-3124
800-492-7122 *Ext.* 3124
Susan.Lee@senate.state.md.us

*February 25, 2021*

Senate Judicial Proceedings Committee

**Senate Bill 623 - Criminal Law - Crimes Involving Computers - "Ransomware"**

Senate Bill 623 mitigates the growing threat of cybercrime in Maryland by defining the crime of ransomware and applying that crime to the unlawful possession of ransomware software with the intent to deploy the technology for malicious purposes. Ransomware is software or a program that prevents victims from accessing computer systems or records until the victim makes a payment to the perpetrator, usually involving untraceable Bitcoin transactions.

Maryland State and local government agencies have fallen victim to high-profile ransomware attacks in recent years. In May of 2019, Baltimore City employees were unable to access online accounts and city payment systems were down for weeks, resulting in some $18 million in restoration and repair costs for the City. These attacks are not only costly, they also threaten public safety. In 2018, a separate ransomware attack rendered Baltimore City's computer-assisted 9-1-1 dispatcher system inoperable for almost a full day.

It's not just big city governments that are targeted with ransomware, local police departments, public and private educational institutions, hospitals and other critical infrastructure face attacks on a daily basis across our State. Some public institutions are targeted not only because they will pay the ransom, but so that the attack itself will generate interest in the software. If an attack garners enough media attention, the software can be marketed and sold on the dark web either as a contract hire or transfer of the ransomware program itself. Private institutions are much more likely to pay to avoid embarrassment, but public institutions have more transparency

requirements that make the damage more severe as they have a greater disincentive to pay off the extortionists.

No business, organization, or industry, no matter the size, is safe from ransomware attacks today. It doesn't take a sophisticated crime syndicate to perpetrate an attack. Any individual connected to the internet has the power to access and utilize crippling ransomware. As the software is disseminated more widely, opportunists like disgruntled employees will deploy these weapons with greater frequency. We must snip this supply growth by fighting demand.

Let me be clear: ransomware is a weapon. This software is a loaded gun with no possible defensive purpose; we shouldn't have to wait for someone to pull the trigger to take decisive action. Law enforcement should be empowered to act against individuals and organizations who possess such weapons without a legitimate purpose *before* they are unleashed to wreak havoc on our schools, hospitals, police departments and businesses. That is exactly what this bill does.

Under SB 623, persons who possess ransomware with an intent to use it for anything other than a lawful purpose are guilty of a misdemeanor offense and will face penalties of up to 3 years (down from 10 in last year's version) and/or a $10,000 maximum fine. Additional tweaks to the penalties reflect feedback we received from the chair last session, and I believe it to be well balanced. In addition to the change of the penalty for possession of ransomware with intent to use it, I have brought back some provisions from previous versions of this bill. The private right of action provision is restored, and local school systems as well as hospitals are added to the critical infrastructure category. After the attack on Baltimore County schools this seems reasonable in the age of COVID and remote learning. Going forward systems for schools are going to be that much more important to protect.

Iterations of this bill have been introduced in prior sessions with the support of the Maryland Cybersecurity Council, on which I serve, and this version continues to enjoy the support of the Council. In past years, this legislation has failed to move forward due to minor technical concerns expressed by the former Chairman. SB 623 has been adjusted to confront those concerns in order to create the best conditions for passage.

While we have a lot more work to do as a committee, as a legislature, and as a State to address ransomware attacks and other cybercrime, this bill is a step in the right direction towards strengthening our cybercrime deterrence. Prosecutors and investigators who discover ransomware and the intent to use it, should not be prohibited from preventing a harmful crime from occurring. There is no lawful purpose to have ransomware if you are not doing research, and we should not allow individuals to trade these weapons online until we create weapons of mass destruction without a deterrence structure.

The private sector should also be more transparent about their attacks, and they should expect future legislation to prevent their payment of ransoms to support organized criminals or opportunists. However, SB 623 is a first step toward preventing access to dangerous weapons that have already been targeted against our democratic institutions and the services government provides to citizens and residents. Most of these services now contain a digital component that can be compromised far too easily with this technology that proliferates unabated.

For these reasons, I respectfully request a favorable report on SB 623.

# MCPA-MSA_SB 623_Crimes Involving Computers-Support

Uploaded by: Mansfield, Andrea

Position: FAV

# Maryland Chiefs of Police Association
# Maryland Sheriffs' Association

MEMORANDUM

TO: The Honorable William C. Smith, Jr. Chairman and
Members of the Judicial Proceedings Committee

FROM: Chief David Morris, Co-Chair, MCPA, Joint Legislative Committee
Sheriff Darren Popkin, Co-Chair, MSA, Joint Legislative Committee
Andrea Mansfield, Representative, MCPA-MSA Joint Legislative Committee

DATE: February 25, 2021

RE: **SB 623 - Criminal Law – Crimes Involving Computers**

POSITION: **SUPPORT**

The Maryland Chiefs of Police Association (MCPA) and the Maryland Sheriffs' Association (MSA) SUPPORT SB 623. This bill provides additional protections for health care facilities and public schools with respect to ransomware.

The current law makes it a crime to access another's computer system or copy or attempt to possess the content of a database without authorization of the owner. The current law also prevents a person from causing the malfunction or interruption of the operations of a computer system and certain unauthorized actions involving another's computer system. The current law also prohibits taking those actions against the State government and quasi-public entities with the intent to interfere with their functions.

Recent events have shown that there is a need to extend those protections to health care facilities and public schools by also making it a crime to interfere with their functions by corrupting their computer systems. Recently hospitals and public school systems have become the victims of malicious actors seriously interfering with operation of a large school system and the education of children and impeding hospitals from providing health care and schools teaching students. Such criminals may have different motives for their actions but clearly one is financial gain by holding their victim's hostage unless they pay large sums of money to regain access to their computer systems and records. This bill also addresses the use of ransomware for profit and by making it a crime to possess ransomware with the intent of introducing it into a computer system without authorization of the owner punishable by 3 years imprisonment and a $10,000 fine. As a further deterrent, the bill establishes a civil action for violations of the ransomware sections.

For these reasons MCPA and MSA SUPPORT SB 623 and urge a FAVORABLE committee report.

532 Baltimore Boulevard, Suite 308
Westminster, Maryland 21157
667-314-3216 / 667-314-3236

**HB425 - SB623 - Ransomware.pdf**
Uploaded by: Niemann, Doyle
Position: FAV

MSBA
MARYLAND STATE
BAR ASSOCIATION

St., Baltimore, MD 21201
800-492-1964
| tdd 410-539-3186

**To:** Members of The House Judiciary Committee and Senate Judicial Proceedings Committee

**From:** Doyle Niemann, Chair, Legislative Committee, Criminal Law and Practice Section

**Date:** February 1, 2021

**Subject:** **HB425 – SB623 – Crimes Involving Computers (Ransomware)**

**Position**: **Support**

The Legislative Committee of the Criminal Law & Practice Section of the Maryland State Bar Association (MSBA) **Supports HB425 – SB623 – Crimes Involving Computers (Ransomware)**.

This bill bans the possession of ransomware, which is defined in the bill, with the intent to introduce it into a computer, network or system. It adds health care facility and public school to the list of entities protected and lowers the threshold for classification as a felony.

Ransomware is a growing problem with far-reaching consequences. It has affected multiple entities in Maryland, including major health care facilities, governmental entities, and even the Office of the Public Defender. This is a useful extension of the current law.

The ban on possession of ransomware with intent to use is particularly useful as it will allow law enforcement agencies to act before the harm has been caused.

For the reasons stated, we **Support HB425 – SB623 – Crimes Involving Computers (Ransomware).**

If you have questions about the position of the Criminal Law and Practice Section's Legislative Committee, please feel free to address them to me at 240-606-1298 or at doyleniemann@verizon.net.

Should you have other questions, please contact The MSBA's Legislative Office at (410)-269-6464 / (410)-685-7878 ext: 3066 or at Richard@MSBA.org.

## SB 623- Criminal Law - Crimes Involving Computers-

Uploaded by: Witten, Jennifer

Position: INFO

Maryland
Hospital Association

February 25, 2021

To: The Honorable William C. Smith Jr., Chair, Senate Judicial Proceedings Committee

Re: Letter of Information - Senate Bill 623 - Criminal Law - Crimes Involving Computers

Dear Chair Smith:

On behalf of the Maryland Hospital Association's (MHA) 60 member hospitals and health systems, we appreciate the opportunity to comment on Senate Bill 623.

The health care sector nationwide and in Maryland continues to be targeted by cyber criminals, particularly during the COVID-19 public health emergency.[1] Data breaches target hospitals' cache of personal and financial data for patients and employees. Maryland hospitals appreciate efforts to improve cybersecurity and target ransomware, which accounts for 85% of all malware attacks in the health care field.[2]

Hospitals adhere to the highest standards to protect patient information. Federal law requires routine security risk assessments to ensure hospitals protect against cyberattacks. Yet, including ransomware as a crime in state statute may impede federal agencies, including the FBI and CIA, that oversee cybercrime and prosecute cyberattacks.

As critical infrastructure organizations dedicated to safety and health, hospitals are committed to strengthening our defense against cyberattacks. If the committee proceeds with this bill, we ask that the committee consider ***clarifying*** within the bill that civil action ***shall only*** be brought against the perpetrator of the cyberattack—rather than other parties.

For these reasons, we abstain from recommending a position on SB 623 and *request clarification* of the civil action provision should the sponsor and committee move this bill forward.

For more information, please contact:
Jennifer Witten, Vice President, Government Affairs
Jwitten@mhaonline.org

[1] Cybersecurity and Infrastructure Security Agency. (November 2, 2020). "Alert (AA20-302A):Ransomware Activity Targeting the Healthcare and Public Health Sector"
[2] Verizon. (2018). "2018 Data Breach Investigations Report."