

**Joint Legislative Committee on Technology and Cybersecurity**

Minutes of Meeting  
2021 Interim  
November 18, 2021

**I. CALL TO ORDER**

Representative Barry Ivey, chairman of the Joint Legislative Committee on Technology and Cybersecurity, called the meeting to order at 9:23 a.m. in House Committee Room 4, in the state capitol in Baton Rouge, Louisiana.

**II. ROLL CALL**

**HOUSE MEMBERS PRESENT:**

Representative Barry Ivey  
Representative Richard Nelson

**HOUSE MEMBERS ABSENT:**

Representative Daryl Deshotel  
Representative Kyle Green  
Representative Matthew Willard

**SENATE MEMBERS PRESENT**

Senator Barry Milligan  
Senator Ed Price  
Senator Mike Reese  
Senator Gary Smith

**SENATE MEMBERS ABSENT:**

Senator Stewart Cathey

**HOUSE STAFF MEMBERS PRESENT:**

Amy Pirtle, committee attorney  
Zachary Gonzalez, central staff attorney  
Jennifer Watson, committee administrative  
assistant  
Robert Singletary, division director

**SENATE STAFF MEMBERS PRESENT:**

Monique Appeaning, committee legislative  
fiscal analyst

**ADDITIONAL HOUSE ATTENDEES  
PRESENT:**

Myrtis Jarrell, sergeant at arms

**ADDITIONAL SENATE ATTENDEES  
PRESENT:**

Edna Buchanan, sergeant at arms

### **III. PRESENTATION BY THE OFFICE OF TECHNOLOGY SERVICES (OTS)**

Neal Underwood, deputy chief information officer, Division of Administration, OTS, 1201 North Third Street, Baton Rouge, LA 70802, (225) 342-7105, gave an overview of OTS operations.

Mr. Underwood described how OTS protected information about businesses and citizens and provided services for infrastructure, benefits, healthcare, and law enforcement. He said identity theft is the number one threat. He cited the following statistics: 37,000 employees use state technology; there are 5,000 data servers; there are 800 locations in and outside of the state; out of 300 million emails each year, one million were rejected; 625 million connections were rejected each day; 3.2 billion events took place daily in Louisiana; and the number one threat was user error.

Representative Ivey asked where reinforcing data infrastructure was most needed. Mr. Underwood said that 80% of funds from the federal infrastructure act were earmarked for the benefit of local government. One challenge of OTS was to recruit professionals at the state and local levels.

Mr. Underwood recalled the 2019 ransomware threat at K-12 schools. Restoration efforts were performed in seven school districts and preventative efforts were performed for neighbors of the school districts.

Representative Ivey asked if there was cybersecurity scalability. Mr. Underwood answered that Louisiana has been on the forefront of that issue by necessity. Just as for natural disasters, Louisiana built response teams for electronic events. He said OTS built infrastructure that provided assistance to local governments. The model was already built between states and the federal government. The federal government sponsored a multi-state consortium, MS-ISAC, where everyone exchanges threat information. If Louisiana received a threat, it was shared with the federal government, which shared it with other states.

Representative Ivey asked what Governor Edwards has done with cyber security. Mr. Underwood replied that through the National Governors Association, Louisiana worked with the response model as an emergency function. The Governor's Office of Homeland Security and Emergency Preparedness had a list of emergency functions, and OTS added cybersecurity event response to the list. A cybersecurity council was created by executive order. Mr. Underwood noted that the work of OTS was never done because the world keeps changing.

Representative Ivey inquired about competitiveness of pay. Mr. Underwood answered that OTS had training programs that produced talent for entry-level jobs with room for growth, including a partnership with the Louisiana National Guard. Entry level paid \$60,000 - \$70,000 in the state, but an entry level job in cybersecurity in the private sector paid \$80,000-\$90,000. Competent practitioners were paid above six figures. OTS can contract resources at expert levels that it cannot afford to hire.

Witness cards submitted by individuals who did not speak are as follows: 2 in support. Witness cards are included in the committee records.

#### **IV. DISCUSSION ON CYBERSECURITY**

Representative Ivey offered a motion to enter executive session. Without objection, the motion passed by a vote of 6 yeas and 0 nays. Representatives Ivey and Nelson, and Senators Milligan, Price, Reese, and Smith voted yea.

Cybersecurity events were discussed in executive session in accordance with R.S. 42:18(A)(4) at 10:14 a.m.

The committee adjourned executive session at 12:03 p.m.

#### **V. DISCUSSION ON SENATE RESOLUTION NO. 188 OF THE 2021 REGULAR SESSION**

Senator Reese introduced Ryan Harkins, senior director of public policy, Microsoft, 309 Settlers Trace, Lafayette, LA 70508, (337) 278-4871.

Mr. Harkins stated that in 1995 the European Union passed a data protection directive. This directive was updated when the European Union passed the General Data Protection Regulation (GDPR). In 2019, California passed the California Consumer Privacy Act (CCPA). Virginia and Colorado passed similar laws.

Mr. Harkins said data privacy means consumers should: (1) control their own data, including the right to transparency; (2) understand what companies are collecting about them; (3) know what businesses are doing with the information; (4) have the right to access their personal data; (5) have the right to correct data if it's incorrect; (6) have the right to request that their data be deleted; and (7) have the right to exercise some form of choice or consent about practices that pose risks to privacy.

Mr. Harkins said companies have a duty to specify the purpose for which they are going to collect and use data, provide limits on secondary use of data, conduct assessments, and make data available for review by other parties.

Representative Ivey asked what the standard was. Mr. Harkins replied that the Virginia and Colorado laws were good starting places. These laws were drafted better and were much easier to understand and comply with because they required companies to be responsible stewards of the data they collect.

Mr. Harkins said that in 2007, researchers at Carnegie Mellon studied the time it would take the average American to read all the privacy policies encountered in the course of a year. The answer was 76 working days.

Representative Ivey asked if there was accountability for businesses. Mr. Harkins replied that in Colorado and Virginia, enforcement authority was given to the attorney general.

Senator Smith asked why it had been difficult to pass these laws in other states. Mr. Harkins said enforcement and a private right of action were the biggest issues. Mr. Harkins said that California's law contained a right to delete personal information, but it was the most narrow definition of the three laws that had passed. California's data deletion laws did not apply to data purchased from a data broker or obtained from a source other than the user. In Virginia, the right to delete law applied to not only a user but also to data a company bought from a data broker. In Colorado, deletion rights applied to all three: data collected from a user, data purchased from a data broker, and inferences that were derived about the user.

Senator Smith mentioned the challenge of private business versus government interference and asked what Microsoft was doing to self police.

Mr. Harkins said the U.S. traditionally enacted sector-specific or issue-specific laws like HIPAA to address medical privacy, or COPPA to address children's online privacy. The European Union uses the GDPR, an omnibus approach to privacy based on the United States law of fair information practice principles. He said it wasn't practical to ask a local dry cleaner, pizza shop, or bar to be burdened with a new complex regulatory structure but it was important for companies that did business outside of the country.

Senator Smith said businesses wouldn't operate here if the bill passed in Louisiana because they didn't have to comply in other states. He asked if businesses were coming to the United States because it does not have burdens and limitations on data privacy. Mr. Harkins replied that he was not aware of any companies that did not want to do business in Europe because of data protection laws.

Representative Nelson asked about the practical impact and the cost of compliance. Mr. Harkins said he had seen proposals that required companies to opt-in for all data collection and use. He said those proposals were misguided for a number of reasons, such as consent fatigue. He said policymakers could discuss which role consent would play within a data protection framework. A separate conversation would be standards for consent using a universal consent mechanism.

Mr. Harkins said if the bill would mandate consent for any activity and for those activities the standard would be to opt out and have global privacy control, consumers could just press one button, one time, to opt out. The practical effect of doing that was to provide consumers with more control over their personal information and its use. He said the cost of compliance would depend on the

size of the operation. Mr. Harkins concluded that globally, there were a lot of services that collected a lot of data. He said the size of the company did not always relate to the scope or significance of the privacy harms that could result from data collection activities.

Representative Ivey asked if the U.S. had regulations on data privacy. Mr. Harkins said there had not been comprehensive privacy laws, but there were consumer protection laws to prohibit unfair deceptive trade practices. Representative Ivey asked who the stakeholders of this bill would be. Mr. Harkins said he didn't know, but if a person had a business today, that business would likely have a web presence for collecting data about people and be subject to privacy law issues.

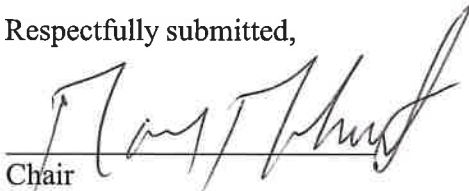
## **VII. OTHER BUSINESS**

There was no other business.

## **VIII. ADJOURNMENT**

The meeting was adjourned at 1:09 p.m.

Respectfully submitted,



Chair

Joint Legislative Committee on Technology and Cybersecurity

Date approved: 02-25-25

The committee has acknowledged on 02-25-25 that these minutes were prepared in accordance with the rules of the House of Representatives.