THE DEVELOPMENT OF CURRENT DIGITAL FORENSICS POLICIES AND FEDERAL LEGISLATION

by

KATHERINE VREELAND SNYDER

B.S, Rochester Institute of Technology, 2017

A thesis submitted to the

Faculty of the Graduate School of the

University of Colorado in partial fulfillment

of the requirements for the degree of

Master of Science

Recording Arts Program

2021

This thesis for the Master of Science degree by

Katherine Vreeland Snyder

has been approved for the

Recording Arts Program

by

Catalin Grigoras, Chair

Cole M. Whitecotton

Katherine A. Hansen

Date: May 15, 2021

Snyder, Katherine Vreeland (M.S., Recording Arts Program)

The Development of Current Digital Forensics Policies and Federal Legislation

Thesis directed by Associate Professor Catalin Grigoras

ABSTRACT

The last few years have shown a rapid technological development in the digital evidence and cybersecurity industries. This paper discusses the chronology of four recent pieces of federal legislation from the beginning of the respective industry through the federal bill being passed. The four laws discussed are the American Innovation and Competitiveness Act, the Strengthening State and Local Cyber Crime Fighting Act of 2017, the IoT Cybersecurity Act of 2020, and the IOGAN Act. Each chapter covers the industry's history, the scientific community's validation and authentication of the industry, related standards, associated previous state and federal laws, and a discussion of what the law entails. The purpose of this paper is to highlight federal digital evidence based legislation and accentuate the work of the scientific community so that the two may have a more symbiotic relationship in the future.

The form and content of this abstract are approved. I recommend its publication.

Approved: Catalin Grigoras

DEDICATION

This paper is dedicated to Kevin, I would not have been able to do all of this without you (and all the coffee that magically appeared on the desk next to me). Thank you for all of your help, love, and sacrifice so that I can do what I love.

I would also like to dedicate this paper to my wonderful parents, Tracey, Jon, and Christine, whose support means the world to me. Thank you for always pushing me to be the best I can be and encouraging me to follow my heart.

While she may no longer be with us, this paper is also dedicated to my grandmother, Jessie. She passed away ten days after I received my acceptance to this program and was thrilled that I was also pursuing a career in the scientific field. Thank you Gramalee for your support and for smashing the glass ceiling in the early days of DNA research.

ACKNOWLEDGEMENTS

I would like to express my gratitude to the wonderful staff at NCMF for all of the hard work they have put into the program. Their guidance, encouragement, and unwavering commitment allowed me to develop a strong knowledge base on which to build my career.

Cathee Hansen, your continued support and mentorship over the years has meant the world to me. You have helped me to bridge the gap of understanding between academia and the professional world.

To my wonderful cohort: I will always cherish all of the laughs, support, and memories that we shared. I can't wait to see where you all take your newfound knowledge.

A great big thank you to each and every one of you!

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

AICA – American Innovation and Competitiveness Act

ASCLD – American Society of Crime Laboratory Directors

ASTM – American Society for Testing and Materials (Now known as ASTM International)

America COMPETES Act – America Creating Opportunities to Meaningfully Promote Excellence in Technology, Education, and Science Act

BJA – Bureau of Justice Assistance

DARPA – Defense Advanced Research Projects Agency

DMCA – Digital Millennium Copyright Act

DME – Digital and Multimedia Evidence

DNC – Democratic National Committee

DOJ – Department of Justice

ECPA – Electronic Communications Privacy Act of 1986

ENSIA – European Network and Information Security Agency (now known as European Union Agency for Cybersecurity)

GAN – Generative Adversarial Network

IBM – International Business Machines Corporation

IOGAN Act – Identifying Outputs of Generative Adversarial Networks Act

IoT – Internet of Things

IP – Internet Protocol

IRS – Internal Revenue Service

ISP – Internet Service Provider

NASA – National Aeronautics and Space Administration

NCFI – National Computer Forensics Institute

NIST – National Institute of Standards and Technology

NSF – National Science Foundation

OMB – United States Office of Management and Budget

STEM – Science, Technology, Engineering, and Mathematics

SWGDE – Scientific Working Group on Digital Evidence

USSS – United States Secret Service

CHAPTER I

INTRODUCTION

As new technological fields emerge, the digital forensics community has quickly adapted and developed strategies to deal with new devices and their associated issues. Typically, the forensics community follows a specific order for dealing with new concepts: they begin with analyzing and authenticating pieces of the emerging industry, and then organizations like the Scientific Working Group on Digital Evidence write best practices and guidelines for how to manage the devices as they become more prevalent. Once these documents are accepted by the scientific community, legislation is written, often at a state level. Sometimes the state laws are passed or something happens that garners national attention, and a federal bill is written and voted on (1). Once this occurs, the details outlined in the law are implemented, and several months or years later, related casework can be seen in the court system.

The chronology outlined in this paper is from a purely forensics perspective, as the political chronology of the bills covered is not as relevant to the National Center for Media Forensics. This paper examines the evolution of four laws in response to technological evolution. This helps scientists and developers to be better informed about the regulations they face and the role they themselves play in the development of new legislation. By understanding the past, new technology can be presented in a way that legislation can be formed around it. Since science needs to be backed up by law, having the reliability and credibility of the scientific community when creating new technology smooths the legislative process. Past years have had a disconnect between the development of technology and the legislation that accompanies it.

Recent years have shown rapid technological development, and related legislation has only recently begun to catch up. Laws tend to lag significantly behind the industry's advances,

largely because most legislation has been reactionary - it is passed in response to a high-profile incident or case. Being able to develop new technology in a manner that allows for proactive legislation would greatly benefit both the legal system and the field of digital forensics.

Previous Legislative Proposals

Historically, several technology-based bills have been drawn up but have not passed one or more sections of Congress. Most recently, the Technology in Criminal Justice Act of 2019 did not receive a vote by the time the 116th Congress concluded. When this occurs, the bill is removed from consideration and must be reintroduced in the new session of congress. The Technology in Criminal Justice Act of 2019 (also known as H.R. 5227) aimed to create the "Office of Digital Law Enforcement" within the DOJ and to use this new office to train and support criminal justice personnel. It also would have designated a "Center of Excellence for Digital Forensics" within the DOJ for training, research, and review of all training programs currently in existence (2). This bill was referred to the Subcommittee on Crime, Terrorism, and Homeland Security, which determined that the Strengthening State and Local Cyber Crime Fighting Act of 2017 (H.R. 1616) was sufficient.

Another bill that was introduced but not signed into law was H.R. 8239, also known as the Forensic Science Research and Standards Act of 2020. This bill aimed to facilitate the creation and dissemination of forensic science standards by establishing the Organization of Scientific Area Committees for Forensic Science within NIST. While it covered several different types of forensic science, it specifically aimed to address "digital and multimedia, or any successor thereto, [and] shall develop standards for validating or assessing the authenticity of digital content, including content created by technologies that synthesize or manipulate digital

content such as deepfakes (3).” H.R. 8239 also went to the Senate where it was reported on, but the bill did not receive a vote in either the House of Representatives or the Senate.

Even though the above bills did not become law, they show that there is a growing need for digital forensics legislation. While digital forensics technology is developing rapidly, the legislation that accompanies it is not keeping pace, despite previous attempts to bring the legal system up to speed. With a more collaborative relationship between law makers and scientists, legislation can be formed while the technology is being developed. This would remediate the issue of lagging legislation and create a more just legal system. Each of the following chapters covers a digital forensics bill, from industry nascence to becoming law.

CHAPTER II

AMERICAN INNOVATION AND COMPETITIVENESS ACT

History and Previous Legislation

Science, technology, engineering, and mathematics (STEM) fields have been around since ancient times, and people have been educating each other on the topics since the dawn of history. The STEM-based field of forensic science dates to Greek and Roman societies, where autopsies were conducted on the recently deceased to determine cause of death. Centuries later, scientists began testing blood samples to determine if they were human or animal, and if blood found at a crime scene was the same blood type as the suspect. Roughly at the same time, fingerprinting methods were developed to aid in identifying who was at the crime scene, garnering more widespread interest in the forensic sciences (4). While blood testing and fingerprinting are common practice now, they were revolutionary when first introduced. That introduction came from a solid scientific understanding that evolved into standard practice through education. With education and public interest, STEM, forensic sciences, and other related fields have the opportunity to grow and advance.

While there has been interest in the broader field of STEM for centuries, the creation of the popular fictional character Sherlock Holmes introduced the field of forensic sciences to the general public. This, coupled with development of NASA in 1958, led to a greater national interest in science and a renewed curiosity of what could be discovered.

The need for a digital forensics field became more obvious in the second half of the twentieth century. IBM's personal computer led to an explosion of computer hobbyists, including law enforcement personnel from agencies across the country. Since they understood that computers and related technology would soon be a critical component in criminal

investigations, the law enforcement personnel formed the International Association of Computer Investigative Specialists. In 1993, the FBI hosted the first International Conference on Computer Evidence in Quantico, Virginia, which left attendees in agreement that the scientific community needed to join forces to provide each other with assistance, experience, and cooperation to maximize the positive outcomes of early computer forensics cases. Many investigative tools were home grown, and examiner training was eventually offered by these pioneers because the demand far outweighed the available examiners' capacity. Eventually, digital forensics became an accepted scientific practice and the number of examiners grew, however it could be argued that today there are still not enough for the influx of digital forensics cases (5). Seeing this, the digital forensics community decided to develop a standard curriculum for examiners, including the ASTM Standard Guide for Education and Training in Computer Forensics. Given the rapid acceleration of technological development, reports indicated that it would be beneficial for the United States to establish a national curriculum for STEM education to remain competitive in the international arena.

In 2007, the National Academy of Sciences, National Academy of Engineering, and Institute of Medicine released a report titled "Rising Above the Gathering Storm: Energizing and Employing America for a Brighter Economic Future". This report stated that America was falling woefully behind other countries in terms of STEM education, and a coordinated federal effort was needed to regain the pre-eminence in the fields of science and technology that the United States once had (6). This prompted Barton Gordon, a U.S. Representative from Tennessee, to write the original America COMPETES Act.

The America COMPETES Act was signed into law on August 9th, 2007, by George W. Bush. Its goal was to invest in innovative scientific fields through research and development with

the hopes that new discoveries would improve the competitiveness of the United States. It also "aimed to set a national policy for investment in research and development that maintains the competitiveness and international leadership of the United States (7)." It had several provisions to fund education and the National Science Foundation. The Act was reauthorized in 2010 and was the subject of contentious debate until 2017, when it was supplanted by the American Innovation and Competitiveness Act (AICA).

Several other STEM education bills were introduced between 2015 and 2016. These included the Crowdsourcing and Citizen Science Acts of 2015 and 2016, and the Science Prize Competitions Acts of 2015 and 2016. The Networking and Information Technology Research and Development Modernization Act of 2016 was also introduced. Only the Science Prize Competitions Act of 2016 was signed into law, but each bill was taken into consideration when writing the AICA.

The American Innovation and Competitiveness Act was the culmination of hard work by legislators, educators, and scientists. Not only did it encompass general K-12 education requirements, but it also stressed the importance of forensic science research and progress. By incorporating the STEM education bills discussed above, AICA has cemented the growth and competitiveness of the United States for years to come.

The Forensic Community's Approach to Education

The forensic community has long embraced STEM education and encourages it for all examiners. SWGDE has released several training guidelines and error mitigation strategies, including the SWGDE/SWGIT Guidelines & Recommendations for Training in Digital & Multimedia Evidence released in 2010. This paper outlines different types of training, how frequently training should be assessed, and what types of training are needed for a variety of

digital evidence based fields (8). Later, SWGDE released core competency guidelines for mobile phone forensics, audio examinations, and embedded device forensics. These core competency papers suggested a basis for training and proficiency testing to verify that examiners are properly trained in each subject. General proficiency testing guidelines were then established and aimed to provide a defined level of expertise for all DME examiners. Finally, in 2016 the SWGDE Training Guidelines for Video Analysis, Image Analysis and Photography were released, which recommends topics and training guidelines for video analysis, image analysis, and photography (9).

ASTM also has released training guidelines titled "Standard Guide for Education and Training in Computer Forensics" or ASTM E2678. This guide discusses computer forensics-specific training, as ASTM does not consider audio, imaging, and video forensics to be subdisciplines of computer forensics as other organizations do. It outlines curricula for programs ranging from untraditional education routes to graduate degrees and addresses continuing education needs for examiners (10).

S.3084

The American Innovation and Competitiveness Act was signed into law on January 6th, 2017 by Barack H. Obama after being introduced by Cory Gardner of Colorado. This federal law focuses mainly on the cybersecurity and cryptography sectors but also touches on high-energy physics, fusion energy sciences, and radiation biology. It strongly encourages citizen science as well as a renewed focus on STEM education. It also dictates that a Director of Security position is to be created at NIST.

The Networking and Information Technology Research and Development program received several upgrades through this law. Most notably, it was to coordinate advanced

computer research across several U.S. Government agencies, and it also had its requirements revisited and updated to align more with current trends in the program. The Office of Management and Budget was also directed to create an interagency working group to reduce the burden of administrative matters on federally-funded researchers (11).

One year after passing AICA, the Senate Commerce, Science, and Transportation Committee held a hearing called "One Year Later: The American Innovation and Competitiveness Act." This hearing discussed how the increased funding to NSF and NIST led to an increase in IoT device research, as well as the fields of advanced manufacturing, artificial intelligence, the bioeconomy, cybersecurity, disaster reliance, quantum technology, and technology transfer (12). NIST made great strides in IoT research in particular, developing standards and guidelines for the cybersecurity of interconnected devices. NSF has also increased its oversight and accountability for large facilities and has greatly increased its support for medium-sized projects. Additionally, NSF set aside an annual budget for K-12 computer science education to make America an international competitor for years to come.

CHAPTER III

STRENGTHENING STATE AND LOCAL CYBER CRIME FIGHTING ACT

History, Previous Legislation, and Recent Issues

Cybercrime has been a burgeoning issue for years at the federal, state, and local levels. Since the days of phone hacking in the 1970s, criminals have been using advanced knowledge to gain entry into computer systems they are not authorized to enter. Once entry is gained, these criminals may steal money, commit espionage, or engage in other nefarious activities. Despite what high-profile federal attacks like the Russian DNC hackings and the IRS attacks of 2015 may indicate, a majority of cybercrime happens at a smaller, local level. Attacks like the one in Oldsmar Florida, where the water supply was compromised with sodium hydroxide, are becoming increasingly common (13). The main issue facing these smaller municipalities is the potential lack of resources and training to deal with a cyber-attack.

For decades, the Federal government has been trying to better equip smaller municipalities with the training and resources needed to deal with attacks on U.S. entities. One of the most expansive laws to do so was the Omnibus Crime Control and Safe Streets Acts of 1968. Sections of this law related to wiretapping were used to write H.R. 1616 (14). These sections limited the information that the government could obtain from its citizens and detailed citizens' protections from unreasonable search and seizure under the fourth amendment.

The Homeland Security Act of 2002 was originally written after the September 11th attacks on the World Trade Center in New York City. It created several new departments and positions within the federal government, the highest profile being the Department of Homeland Security and the presidential cabinet position of Secretary of Homeland Security (15). This law was amended with the passing of H.R. 1616 in 2017 to include the designation of NCFI and to

encourage the education of law enforcement personnel so that they may better understand current cybercrime trends and threats before applying techniques learned at NCFI to their own jurisdictions.

Another piece of legislation that was incorporated into H.R. 1616 is the National White Collar Crime Control Act of 2017. This bill amends the Omnibus Crime Control and Safe Streets Act of 1968 to establish a new section, called the National White Collar Crime Control Act of 2017. This authorized the DOJ's BJA to create a grant to fund training and technical assistance for law enforcement officers, investigators, auditors, and prosecutors to help identify, investigate, and prosecute white collar crime, including child pornography, internet crimes against children, and other high-tech crimes (16).

Community Response and Policies

One of the biggest challenges the digital forensics community faces is the lack of education among those with important enforcement roles, whether this be judges who do not know enough about digital forensics to properly understand the evidence, or officers whose out-of-date information leads to the destruction of evidence. Justice is better served when everyone involved is well-educated on how to handle digital evidence. SWGDE has released several papers on training guidelines, core competencies, and proficiency testing which were discussed in chapter two. Other organizations have also released training guidelines or recommendations, including ENFSI and ASCLD.

In 2015, ENFSI released a document titled “Methodological Guidelines for Best Practice in Forensic Semiautomatic and Automatic Speaker Recognition including Guidance on the Conduct of Proficiency Testing and Collaborative Exercises.” This document covered several topics including how proficiency testing should be performed for forensic semiautomatic and

automatic speaker recognition and the frequency at which testing should occur (17). It also outlines various examples of testing procedures for speaker recognition and details how to approach several issues that may arise during testing.

ASCLD has released a recommendation for the development of a national forensic science curriculum so that criminal justice practitioners like judges and attorneys are better informed about the science. It also suggests that a similar program is needed for law enforcement officers and claims that they are under-equipped for being the first line of preservation for all forms of evidence. The proposed curriculum would be developed by leading experts in the appropriate forensic science field, so criminal justice practitioners could take that information back to their offices and disseminate the best information available to ensure that justice is properly served (18).

H.R. 1616

After being introduced by John Ratcliffe of Texas, H.R. 1616 was signed into law by Donald J. Trump on November 2nd, 2017. This law is also known as the Strengthening State and Local Crime Fighting Act of 2017. It declared that the National Computer Forensics Institute must be created within the U.S. Secret Service to spread information related to the investigation and prevention of cybercrime and potential cybercrime threats. NCFI is also directed to educate and equip a wide variety of law enforcement officials, including state, local, tribal, and territorial law enforcement officers, prosecutors, and judges. NCFI is to educate officers, prosecutors, and judges on current cybercrimes and threats, methods for investigations and examinations, and how to manage digital forensics-based prosecutorial and judicial challenges. Training is to include conducting investigations and forensic examinations of cybercrimes, as well as appropriate responses to network intrusion incidents. Officers, prosecutors, and judges will be trained on

methods to obtain, process, store, and admit digital evidence in court. NCFI will also ensure that cyber-crime related information is shared with officers and prosecutors. NCFI may also provide officers with computer equipment, hardware, software, tools, and manuals needed to conduct investigations and forensic examinations. Finally, NCFI is to expand the network of Electronic Crime Task Forces of the Secret Service by training officers at the NCFI facility (19).

As of early 2021, NCFI continues to educate law enforcement officers and others involved with digital evidence. Currently, it offers courses on a wide variety of digital forensics topics including basic digital forensics, vehicle forensics, mobile phone forensics, undercover online investigations, and digital currency. It also has several specific courses for judges and prosecutors. To take a class, the student must be a full-time employee of a state or local government agency and can apply to the course through their local USSS field office. From there, the student is nominated, and attendees are selected from the nominations six weeks before the course is set to begin (20). Depending on the topic, there are only sixteen or twenty-four students per course and the courses are in very high demand. Unfortunately, courses have been suspended due to the Covid-19 pandemic until future notice, but hopefully they will resume shortly.

CHAPTER IV

IOT CYBERSECURITY ACT

Industry History and Policies

Internet of Things devices have quickly become popular, with products like the Amazon Alexa and Ring cameras becoming household names. Smart devices have been around since 1982, when researchers retrofitted a Coca-Cola vending machine at Carnegie Mellon University with micro-switches that told users if there were drinks present in the machine and how long they had been in the machine (and therefore how cold they were). The researchers could then run a companion status inquiry program from their desks to determine if the machine had cold Cokes waiting for them (21). Current IoT devices have come a long way from Coke machines, and can be defined as the "extension of internet connectivity into physical devices and everyday objects (22)."

Modern IoT devices can be categorized several ways, based on their applications. The most well-known category is comprised of consumer products, which encompasses home automation products and wearable devices. Consumer products also extend to assistive technologies, which help people with disabilities be more independent. One example of this application is a smart fire alarm that can be paired with Bluetooth-enabled hearing aids to alert the wearer when the fire alarm goes off. IoT devices can also be used in industrial and medical applications and are often used in military applications.

However, there are significant concerns about the security of IoT devices, especially given the widespread adoption of the technology. Several studies in the last few years have shown that the number of connected IoT devices is rapidly increasing and is expected to reach

well into the billions by 2025. With the increase in devices comes an increase in security concerns, especially given that many devices lack the security to keep data protected (23).

Several forensics groups have recognized how prolific IoT devices have become and have quickly worked to establish guidelines and best practices. SWGDE has released two papers on IoT devices as of April 1st, 2021.

In 2017, SWGDE published Best Practices for the Acquisition of Data from Novel Digital Devices. This paper outlines how to deal with devices that do not fall under the typical categories of digital devices collected, like mobile devices or computers. This paper specifically categorizes IoT devices as novel devices, since they were not commonplace when the paper was published. It outlines physical examination steps as well as considerations and possible methods to keep in mind for a successful data acquisition (24). It gives seven acquisition methods that could be used with a novel device, ranging from disassembly of the device to expose obscured connection points to acquiring data from other sources like the cloud. Additionally, the paper discusses when each method should be used and important considerations to have the best chance at a successful acquisition.

The most recent SWGDE paper is Technical Notes on Internet of Things Devices, which discusses the possibility of IoT devices containing data, data storage, and general handling of Internet of Things devices. It breaks IoT devices down into eight classes: wearables, smart speakers, sensors, control systems, capture devices, implants, vehicles, and appliances. It then discusses law enforcement's collection of IoT devices, emphasizes the importance of following general evidence collection best practices, and suggests documenting any display screens or device indicators before collection. The SWGDE document then cautions examiners about the volatile nature of IoT data and warns about using any trigger events that may overwrite the data.

Trigger events can include saying a certain phrase like “Hey, Alexa” or walking by a front door that has a video doorbell. Since the majority of data is stored elsewhere, in the cloud or on a personal computer, for instance, improper preservation of the device can cut off access to offsite data (25). The paper further emphasized challenges that may arise from acquisition and examination that should be kept in mind when processing IoT devices.

Since 2019, NIST has published several papers on IoT devices and the cybersecurity risk that they pose to the general public. Two of these papers, “Cyber-Physical Systems and Internet of Things” and “Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks” outline considerations and growth trends of the devices. They discuss how the information technology needs of IoT devices are wildly different from traditional devices, and how many organizations may not be aware of how many IoT devices they possess or the cybersecurity risk that they pose. The latter paper outlines IoT device functions that can be classified in one of three ways: transducing, interfacing, or supporting. Transducing capabilities are the functions that allow humans to interact with the devices, such as sensing that an audio trigger event occurred. Interfacing capabilities are device-to-device responses to trigger events, such as changing the temperature in response to an auditory command. The supporting capabilities would be the functional necessities that happen behind the scenes, like device management and security (26). This paper goes on to suggest security recommendations for all three classifications of IoT device functions and outlines risk mitigation goals to prepare for cybersecurity and privacy risks.

Previous Federal and State Legislation

Since it has become apparent that IoT devices were not merely a passing fad, several states have passed legislation regulating the devices, and three federal bills were introduced to

Congress. Both California and Oregon successfully passed bills prior to 2020 that require manufacturers to equip IoT devices with reasonable security features appropriate to the device.

California was the first state to pass an IoT-based bill, signing SB 327 into law on September 28th, 2018. This law requires the manufacturer of a connected device to have practical security features on the device before it is sold to a consumer. These security features must be "appropriate to the information [the device] may collect, contain, or transmit, and designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure (27)." California defines a connected device as "any device, or other physical object that is capable of connecting to the Internet, directly or indirectly, and that is assigned an Internet Protocol address or Bluetooth address" and manufacturer as "the person who manufactures, or contracts with another person to manufacture on the person's behalf, connected devices that are sold or offered for sale in California (27)." The vague language of the law has led to some confusion as to the level of security features necessary to comply. While this law is broad, it achieves its goal of making connected devices safer for the average consumer's data privacy.

Oregon modeled its law after California's, passing HB2395 on May 22nd, 2019. It is similar to SB 327, with the only notable differences being how "connected device" and "manufacturer" are defined. In Oregon law, a connected device is defined as a device which directly or indirectly connects to the internet, is primarily used for personal, family, or household purposes, and is assigned an IP address. Manufacturer is defined as "a person that makes a connected device and sells or offers to sell the connected device in this state (28)." While these may seem similar to the California definitions, the inclusion of primary usage for personal, family, or household purposes can pose a significant challenge for manufacturers. This is due to

the broad language that is used in the law itself which makes compliance rather difficult, and several cybersecurity experts have suggested that both the California and Oregon laws have too many loopholes in them to be effective (29).

Three federal bills have been introduced to Congress to address IoT devices at a national level. These are the Automatic Listening Exploitation Act of 2019, the Protecting Privacy in Our Homes Act, and the Cyber Shield Act of 2019. The Automatic Listening Exploitation Act of 2019 was introduced in July of 2019 and limited the capture and use of recordings from smart speakers and video doorbells. It specifically limited the capture methods, storage, and dissemination of the recordings. It also dictated that the devices could not always be recording, i.e. the recording must be activated by the user, a sensor, or a trigger event like someone saying "Hey, Alexa" (30). This bill did not come to a vote before the 116th Congress concluded, so it would have to be reintroduced in order to be considered again.

The next bill was the Protecting Privacy in Our Homes Act, which was introduced in September of 2019. This bill also did not come to a vote by the conclusion of the 116th Congress, and therefore is no longer under consideration. It was a limited bill, only requiring that manufacturers disclose if an IoT product had a camera or microphone in it if it was not specifically marketed as a camera or microphone (31). This would affect devices like the Amazon Alexa, which has a microphone to determine what the user is saying but is marketed as a speaker.

The final piece of legislation introduced was the Cyber Shield Act of 2019. The goal of this bill was to create a voluntary program to promote IoT devices which meet industry cybersecurity standards and best practices (32). Like the two bills before it, it did not receive a

vote by the conclusion of the 116th Congress and is no longer under consideration. These bills were the precursors to the IoT Cybersecurity Act of 2020.

H.R. 1668

H.R. 1668, more commonly called the IoT Cybersecurity Act of 2020, was signed into law by Donald J. Trump on December 4th, 2020. The bill requires NIST to create and disseminate standards and guidelines for the federal government regarding agency use and management of IoT devices owned or controlled by a federal agency and connected to information systems owned or controlled by an agency. This includes minimum information security requirements for managing IoT device based cybersecurity risks. It also declares that federally owned IoT devices must adhere to security guidelines, standards, and best practices to increase the cybersecurity of these devices. These must be developed by NIST and be reviewed and revised every five years. NIST must also create guidelines for agencies, contractors, and subcontractor communications to appropriately address security vulnerabilities. The act also states that an agency cannot use or possess an IoT device if it cannot meet the security guidelines, however, there are a few exceptions to this statement. A waiver can be obtained to possess such a device for research purposes, for national security, or when the device is secured using effective alternative methods (22). The law also states that within two years of the bill becoming a law, the OMB must oversee the implementation of the created policies, standards, and guidelines pertaining to the security vulnerabilities of information systems.

Since this bill was signed into law a few months before this paper was written, much of the policy development is still taking place. However, the act declared that NIST standards and guidelines for the federal government on the appropriate use and management of IoT devices must be developed within ninety days of the act being signed into law (22). Four documents have

been released to the public for comment: NIST Special Publication (SP) 800-213 and NIST Interagency Reports (NISTIRs) 8259B, 8259C and 8259D. These documents outline the steps necessary to comply with the NIST requirements, for both manufacturers and purchasers within the federal government. SP 800-213 provides guidance, background, and recommendations for the successful integration of IoT devices into NIST's risk-based cybersecurity methodology for federal systems. The 8259 series has two previously published papers, and all five papers aim to "provide guidance that IoT device manufacturers can use to help organizations implement SP 800-213's recommendations (33)." Given the exponentially growing number of IoT devices, laws and regulations for advanced IoT device capabilities are certain to emerge.

CHAPTER V

IOGAN ACT

Industry History and Community Response

Artificial intelligence has recently made great strides in development, and with that comes new challenges. One of these challenges is the development of deepfake technology, which is a combination of machine learning and artificial intelligence. It gets the name "deepfake" from a combination of the words "deep learning" and "fake". Deep learning is a method of machine learning that uses artificial neural networks to transform data on multiple levels. One notable application of deep learning is generative adversarial networks, which use deep learning to recognize similarities in a set of data to create new data that shares the same characteristics as the original dataset. In the case of deepfakes, GANs are used to create new content that often looks fairly realistic and can be used to deceive the viewer for various purposes.

While deepfakes have been researched at academic institutions since the 1990s, several high-profile incidents catapulted them into the national spotlight and into the forefront of legislators' minds. One major incident was the creation and dissemination of the DeepNude program, which used artificial intelligence to digitally remove the clothing from user-provided pictures of women. This program only worked on female bodies, and artificially added breasts and a vulva to the uploaded images. After national backlash the creator took down the program, but it had been used thousands of times before it was removed (34). In another incident, several viral videos of Nancy Pelosi were altered to make it seem as though she was intoxicated. These videos were slowed down and her speech digitally altered, and the resulting content was viewed over two million times (35). This garnered even more attention when Facebook refused to

remove the video, stating that it did not meet the company's criteria for "manipulated media" but Facebook has since changed its policies. A third viral deepfake depicted Jay-Z rapping a soliloquy from Hamlet. This led to several DMCA takedown attempts by Jay-Z's legal team, all of which were rejected based on fair use under U.S. Copyright law (36).

The forensic community has been keeping a close eye on the increase of deepfakes and manipulated media. SWGDE published a paper in January of 2021 titled "Artificial Intelligence Trends in Video Analysis" which discusses various applications of artificial intelligence and machine learning, as well as outlines forensic community concerns regarding artificial intelligence. One of the main concerns is the rise of deepfakes and GAN imagery, which can lead to defamation and even national unrest. Unfortunately, it also leads to a distrust of digital evidence, since the existence of manipulated media introduces doubt into the minds of the general public.

This SWGDE paper briefly discusses various possible solutions including the DARPA MediFor project, which "developed technologies that would automatically assess the integrity of an image or video file, produce an integrated platform for end-to-end media forensics evaluation, and provide details that will help facilitate decisions regarding the image or video in question (37)." Another possible solution is an expansion of machine-learning-based education for both examiners and prosecutors, so that they may more accurately verify the integrity of the media and be aware of new challenges they may face. This paper also discusses the rise of computer vision applications, which use computer programs to extract scene content information from an image or video to mimic the capabilities of the human visual system. These have many different law enforcement applications including license plate recognition and facial recognition programs.

Previous Federal and State Legislation

One previous federal attempt at a deepfake-based law is the proposed DEEPFAKES Accountability Act. In this instance, DEEPFAKES stands for "Defending Each and Every Person from False Appearances by Keeping Exploitation Subject." This bill was introduced by Representative Yvette D. Clarke of New York on June 12th, 2019. It aimed to combat the spread of disinformation by limiting how deepfake media can be spread. It required watermarks and disclosures on manipulated content while introducing civil and criminal penalties for those who knowingly violate the act or alter the disclosures (38). This bill was referred to the Subcommittee on Crime, Terrorism, and Homeland Security, where it was decided that it was overbroad and would be unenforceable. It did not receive a vote.

While previous federal bills that encompass deepfakes and manipulated content have not been signed into law, there have been several state laws that directly address the issue of GANs and the content that they create. These laws fall into two categories: manipulated political content and manipulated pornographic content.

Two states have banned manipulated political content before an election. Texas has banned all political deepfakes (39), and California has made it illegal to "create or distribute videos, images, or audio of politicians doctored to resemble real footage within 60 days of an election (40)." These laws were passed in September of 2019 and October of 2019 respectively. They aim to prevent some of the false information and manipulated content that can be found around election seasons to ensure a free and fair election.

The manipulated pornographic content laws are less straightforward than the political content laws, but the created pornographic content is far more prevalent. It is estimated that of the deepfakes available online, ninety-six percent are nonconsensual pornography (41).

Nonconsensual pornography is when a sexual photo or video of a person is shared without that person's consent, colloquially known as "revenge porn." In the United States, forty-six states have bans on revenge porn but the language of the laws excludes deepfakes or manipulated content (42). New York, California, and Virginia have laws that include created content under their nonconsensual pornography laws. New York passed a standalone law in December of 2020 which banned deepfake pornography and banned using an actor's likeness in artificial intelligence-based content for up to forty years following their death (43). California passed a bill in October of 2019 which expanded on the original revenge porn statute to include manipulated and deepfaked content (44). Virginia simply expanded a pre-existing revenge porn law to include deepfaked material (45).

Three states have recently attempted to pass deepfake related bills, but Maine, Massachusetts, and Maryland have all failed. Maine had drafted a similar bill to Texas, L.D. 1988, which banned political deepfakes for sixty days before an election (46). Massachusetts unsuccessfully attempted to pass H.3366, which criminalized creating or distributing a deepfake which "would facilitate criminal or tortious conduct (47)." Maryland proposed H.B. 198, which banned political deepfakes for ninety days before an election (48). While all of these failed to become laws, they show an increased awareness of the concerns surrounding deepfakes and a desire to create legislation to address future issues.

S.2904

On December 23rd, 2020, Donald J. Trump signed S.2904 into law. Otherwise known as the IOGAN Act or the Deepfake Act, this bill focused on furthering research into generative adversarial networks. Specifically, it declares that NIST must research and develop the standards and measurements for new tools to examine the functions and outputs of GANs and the content

that they create or manipulate. Another aspect of this law is that the NSF must support research on information authenticity and manipulated content. NSF is also to support research on synthesized content, like the content created by GANs and similar technologies (49).

As of early 2021, not much progress has been made in the research prescribed by this law, as it is still in its infancy. By December 23rd, 2021, the directors of NIST and NSF will each submit a report that discusses the feasibility of working with the private sector on research opportunities. These opportunities would lead to better detection methods of manipulated media including GAN-generated digital content. This report must also discuss any possible policy changes that could allow for better communication between relevant agencies, the private sector, and NSF for the purpose of implementing innovative approaches to detect manipulated content (50).

CHAPTER VI

CONCLUSION

Given the rapidly changing field of technology, there will always be a need for new research and legislation so that the best possible science can reach both the classroom and the courtroom.

An expansion of NCFI is greatly needed to better serve its original purpose outlined in the Strengthening State and Local Cyber Crime Fighting Act of 2017. While it is an important resource, NCFI's limited class sizes and sole location can pose challenges to many potential participants. Many judges and prosecutors remain critically undereducated regarding digital evidence and the scientific methods used in a digital investigation. This can lead to poor decisions, blundered cases, and the potential miscarriage of justice. More NCFI facilities would cater to people who cannot travel or cannot get into the limited class sizes that currently exist at the Georgia facility.

Currently, digital forensics cases often rely on outdated communications acts and wiretap statutes, because the legislation is still lagging behind the technology. As a result, the courtroom is not getting the most effective science possible, which is not fair to any party involved in the case. Relying on outdated wiretap statutes and historic communications acts leads to complications when issuing search warrants and searching the gathered devices. Outdated wiretap statutes are still being used to justify mobile device search warrants, and the Electronic Communications Privacy Act of 1986 is no exception.

The Electronic Communications Privacy Act of 1986, or the ECPA, is frequently referred to in criminal investigations. The ECPA is a three-part law consisting of the Wiretap Act, the Stored Communications Act, and Title Three: Pen Registers and Trap and Trace Devices. The

Wiretap Act expressly prohibits the use of illegally obtained communications as evidence in a court of law, and "prohibits the intentional actual or attempted interception, use, disclosure," or "procure[ment] [of] any other person to intercept or endeavor to intercept any wire, oral, or electronic communication." Under this act, a judge is able to issue a warrant allowing for the legal interception of communications for thirty days if there is probable cause showing that the intercepted communications will likely show that the person is committing an offense (51). The Stored Communications Act addresses the right to privacy of records held by ISPs, particularly "stored wire and electronic communications and transactional records." These include subscriber name, IP addresses, and billing records. The final section of the ECPA addresses pen registers as well as trap and trace devices. Pen registers record all numbers called from a particular phone line. Trap and trace devices record the incoming calls to a particular device. These two devices are often used in conjunction, and typically replace the need for a wiretap. This section dictates that a court order is required for the installation and usage of a pen register or trap and trace device (51). There were several laws that amended the ECPA, the last one being signed into law in 2008. These include the Communications Assistance to Law Enforcement Act, the Patriot Act and its subsequent reauthorizations, and the FISA Amendments Act of 2008. An update to these amendments is greatly needed, as the technology is far more evolved than it was in 2008.

The Telecommunications Act of 1996 was the first major overhaul done to communications laws since 1934 and was the first time that the internet was mentioned in a communication-based law (52). It only briefly discussed mobile devices, which now greatly outnumber wired telephones and are capable of performing considerably more tasks than they were capable of in 1996. The reliance on this outdated law can lead to searches being carried out inappropriately since the devices in question are barely covered in the law. The lack of guidance

from the law could potentially lead to a miscarriage of justice, so it is imperative to have more modern legislation to dictate appropriate search parameters.

Future Legislation

There are three upcoming federal bills that indicate the direction of digital forensics based legislation. They are the American Drone Security Act of 2021, the Promoting Digital Privacy Technologies Act, and the FedRAMP Authorization Act.

The American Drone Security Act of 2021 bans the federal government from using drones manufactured or assembled by certain entities, especially ones with ties to China. It also requires guidelines from NIST to direct users how to deal with the risks associated with processing, storing and transmitting information in a federally owned drone (53). The Promoting Digital Privacy Technologies Act aims to have NSF support more "privacy enhancing technologies" through merit awarded research grants. It also directs NSF to award research grants for "basic research on innovative approaches to the structure of computer and network hardware and software that are aimed at enhancing computer security (54)." The FedRAMP Authorization Act has passed via a vote by the House of Representatives, but awaits a vote in the Senate, where it has gone to the Committee on Homeland Security and Governmental Affairs. It aims to elevate the security of cloud computing products and to enable the Federal Risk and Authorization Management Program to continuously monitor the risk status of cloud computing products (55). The introduction of these bills shows a desire to have legislation develop alongside technology, rather than long after the technology has been widely adopted.

The ever-changing nature of technology poses constant challenges that can only be adequately managed through the unity of the forensic community and ongoing legislative efforts. Future legislative needs include more modern laws regarding smart devices, more rigorous IoT

device laws, and protecting the personal data of consumers using a wide variety of digital devices. While the forensic community has been proactive with their development of best practices and guidelines, the lag in federal laws regarding new technology remains the biggest challenge facing the field of digital forensics today.

REFERENCES

1. "How Laws Are Made: USAGov." How Laws Are Made | USAGov, 2021, www.usa.gov/how-laws-are-made.

2. United States, Congress, Technology in Criminal Justice Act of 2019. 2019.

3. United States, Congress, *Forensic Science Research and Standards Act of 2020*. 2020.

4. Bell, Suzanne. *Crime and Circumstance: Investigating the History of Forensic Science*. Praeger, 2008.

5. Pollitt M. (2010) *A History of Digital Forensics. In: Chow KP., Shenoi S. (eds) Advances in Digital Forensics VI. Digital Forensics* 2010. IFIP Advances in Information and Communication Technology, vol 337. Springer, Berlin, Heidelberg. https://link.springer.com/chapter/10.1007/978-3-642-15506-2_1

6. United States, Congress, National Academy of Sciences, National Academy of Engineering, and Institute of Medicine. *Rising above the Gathering Storm: Energizing and Employing America for a Brighter Economic Future*, The National Academies Press, 2007.

7. United States, Congress, "America COMPETES Act." *Congress.gov*, 2007. U.S. G.P.O. Congress, www.congress.gov/bill/110th-congress/house-bill/2272.

8. Scientific Working Group on Digital Evidence. *SWGDE/SWGIT Guidelines & Recommendations for Training in Digital & Multimedia Evidence in 2010*. 15 Jan. 2010, swgde.org.

9. Scientific Working Group on Digital Evidence. *SWGDE Training Guidelines for Video Analysis, Image Analysis and Photography*. 8 Feb. 2016, swgde.org.

10. ASTM International. "ASTM E2678-09(2014)- Guide for Education and Training in Computer Forensics." *Astm.org*, 2014, www.astm.org/Standards/E2678.htm.

11. United States, Congress, *American Innovation and Competitiveness Act*.

12. "One Year Later: The American Innovation and Competitiveness Act." 2018.

13. Robles, Frances, and Nicole Perlroth. "'Dangerous Stuff': Hackers Tried to Poison Water Supply of Florida Town." *The New York Times*, The New York Times, 9 Feb. 2021, www.nytimes.com/2021/02/08/us/oldsmar-florida-water-supply-hack.html.

14. United States, Congress, *Omnibus Crime Control and Safe Streets Acts of 1968*. 1968.

15. United States, Congress, *Homeland Security Act of 2002*.

16. United States, Congress, *National White Collar Crime Control Act of 2017*.

17. Drygajlo, Andrzej, et al. "Methodological Guidelines for Best Practice in Forensic Semiautomatic and Automatic Speaker Recognition Including Guidance on the Conduct of Proficiency Testing and Collaborative Exercises." Prevention of and Fight against Crime Programme European Commission - Directorate-General Home Affairs, *European Network of Forensic Science Institutes*, 2015, https://enfsi.eu/wp-content/uploads/2016/09/guidelines_fasr_and_fsasr_0.pdf.

18. "Initial Draft Recommendation on Developing a National Forensic Science Curriculum." *Ascld.org*, 2015.

19. United States, Congress, *Strengthening State and Local Cyber Crime Fighting Act of 2017, Public Law 115-76, November 2, 2017*. 2018.

20. "Home." *NCFI*, www.ncfi.usss.gov/ncfi/.

21. Teicher, Jordan. "The Little-Known Story of the First IoT Device." *IBM*, 13 June 2019, www.ibm.com/blogs/industries/little-known-story-first-iot-device/.

22. United States, Congress, *IoT Cybersecurity Improvement Act of 2020*. 2020.

23. Dahlqvist, Fredrik, et al. "Growing Opportunities in the Internet of Things." *McKinsey & Company*, McKinsey & Company, 16 Sept. 2020, www.mckinsey.com/industries/private-equity-and-principal-investors/our-insights/growing-opportunities-in-the-internet-of-things#.

24. Scientific Working Group on Digital Evidence. *SWGDE Best Practices for the Acquisition of Data from Novel Digital Devices*. 21 Feb. 2017, swgde.org.

25. Scientific Working Group on Digital Evidence. *SWGDE Technical Notes on Internet of Things (IoT) Devices*. 17 Sept. 2020, swgde.org.

26. Boeckl, Katie, et al. "Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks." *National Institute of Standards and Technology*, June 2019, https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8228.pdf.

27. California State, Legislature. Senate Bill No. 327. *California State Legislature*, 28 Sep. 2018, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327.

28. Oregon State, Legislature. House Bill 2395. *Oregon State Legislature*, 30 May 2019, https://olis.leg.state.or.us/liz/2019R1/Downloads/MeasureDocument/HB2395/Enrolled.

29. Robertson, Adi. "California Just Became the First State with an Internet of Things Cybersecurity Law." *The Verge*, The Verge, 28 Sept. 2018, www.theverge.com/2018/9/28/17874768/california-iot-smart-device-cybersecurity-bill-sb-327-signed-law.

30. United States, Congress, *Automatic Listening Exploitation Act of 2019*.

31. United States, Congress, *Protecting Privacy in Our Homes Act*.

32. United States, Congress, *Cyber Shield Act of 2019*.

33. Henderson, Sarah. "NIST Releases Draft Guidance on Internet of Things Device Cybersecurity." *NIST*, 9 Feb. 2021, www.nist.gov/news-events/news/2020/12/nist-releases-draft-guidance-internet-things-device-cybersecurity.

34. Hao, Karen. "An AI App That 'Undressed' Women Shows How Deepfakes Harm the Most Vulnerable." *MIT Technology Review*, MIT Technology Review, 28 Jun. 2019, www.technologyreview.com/2019/06/28/134352/an-ai-app-that-undressed-women-shows-how-deepfakes-harm-the-most-vulnerable/.

35. Holmes, Aaron. "A Doctored Video That Makes Nancy Pelosi Appear Drunk Went Viral on Facebook - Again." *Business Insider*, Business Insider, 3 Aug. 2020, www.businessinsider.com/nancy-pelosi-facebook-declines-to-remove-doctored-viral-video-2020-8.

36. Hochberg, Bill. "YouTube Won't Take Down A Deepfake Of Jay-Z Reading Hamlet - To Sue, Or Not To Sue." *Forbes*, Forbes Magazine, 26 Jan. 2021, www.forbes.com/sites/williamhochberg/2020/05/18/to-sue-or-not-to-sue---that-is-the-jay-zs-deepfake-question/?sh=35f2b5fb128b.

37. Scientific Working Group on Digital Evidence. *SWGDE Overview: Artificial Intelligence Trends in Video Analysis*. 14 Jan. 2021, swgde.org.

38. United States, Congress, *Defending Each and Every Person from False Appearances by Keeping Exploitation Subject to Accountability Act of 2019*.

39. Texas State, Legislature. 86(R) SB 751. *Texas State Legislature*, 01 Sep. 2019, https://capitol.texas.gov/tlodocs/86R/billtext/pdf/SB00751S.pdf.

40. California State, Legislature. Assembly Bill No. 730. *California State Legislature*, 04 Oct. 2019, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB730.

41. The State of Deepfakes: Landscape, Threats, and Impact, Henry Ajder, Giorgio Patrini, Francesco Cavalli, and Laurence Cullen, September 2019.

42. Hao, Karen. "Deepfake Porn Is Ruining Women's Lives. Now the Law May Finally Ban It." *MIT Technology Review*, MIT Technology Review, 16 Feb. 2021, www.technologyreview.com/2021/02/12/1018222/deepfake-revenge-porn-coming-ban/.

43. New York State, Legislature. S5959D. *New York State Legislature*, 30 Nov. 2020, https://www.nysenate.gov/legislation/bills/2019/s5959.

44. California State, Legislature. Assembly Bill No. 602. *California State Legislature*, 04 Oct. 2019, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB602.

45. Virginia State, Legislature. § 18.2-386.2. *Virginia State Legislature*, 11 Feb. 2019, https://law.lis.virginia.gov/vacode/title18.2/chapter8/section18.2-386.2/.

46. Maine State, Legislature. LD 1988. *Maine State Legislature*, 08 Jan. 2020, https://legislature.maine.gov/legis/bills/display_ps.asp?LD=1988&snum=129.

47. Massachusetts State, Legislature. H.3366. *Massachusetts State Legislature*, 11 Nov. 2020, https://malegislature.gov/Bills/191/H3366.

48. Maryland State, Legislature. HB198. *Maryland State Legislature*, 16 Jan. 2021, http://mgaleg.maryland.gov/mgawebsite/Legislation/Details/HB0198?ys=2020RS.

49. United States, Congress, *Identifying Outputs of Generative Adversarial Networks Act*.

50. United States, Congress, *Identifying Outputs of Generative Adversarial Networks Act: Report (to Accompany H.R. 4355) (Including Cost Estimate of the Congressional Budget Office)*.

51. United States, Congress, *Electronic Communications Privacy Act of 1986*. 1987. U.S. G.P.O. Congress.

52. United States, Congress, *The Telecommunications Act of 1996 (P.L. 104-104)*.

53. United States, Congress, *American Drone Security Act of 2021*. 2021.

54. United States, Congress, *Promoting Digital Privacy Technologies Act*. 2021.

55. United States, Congress, *FedRAMP Authorization Act*. 2021.