

# The Legal Space of Cyber Security – More Issues for Research and Practice

## **CAE Cyber Security Forum**

<https://caecommunity.zoom.us/my/caeforum>

**March 14 2018**

**U.S.A.**

Michael Losavio

Jarrold Hinton

Adrian Lauf

Jana Godwin

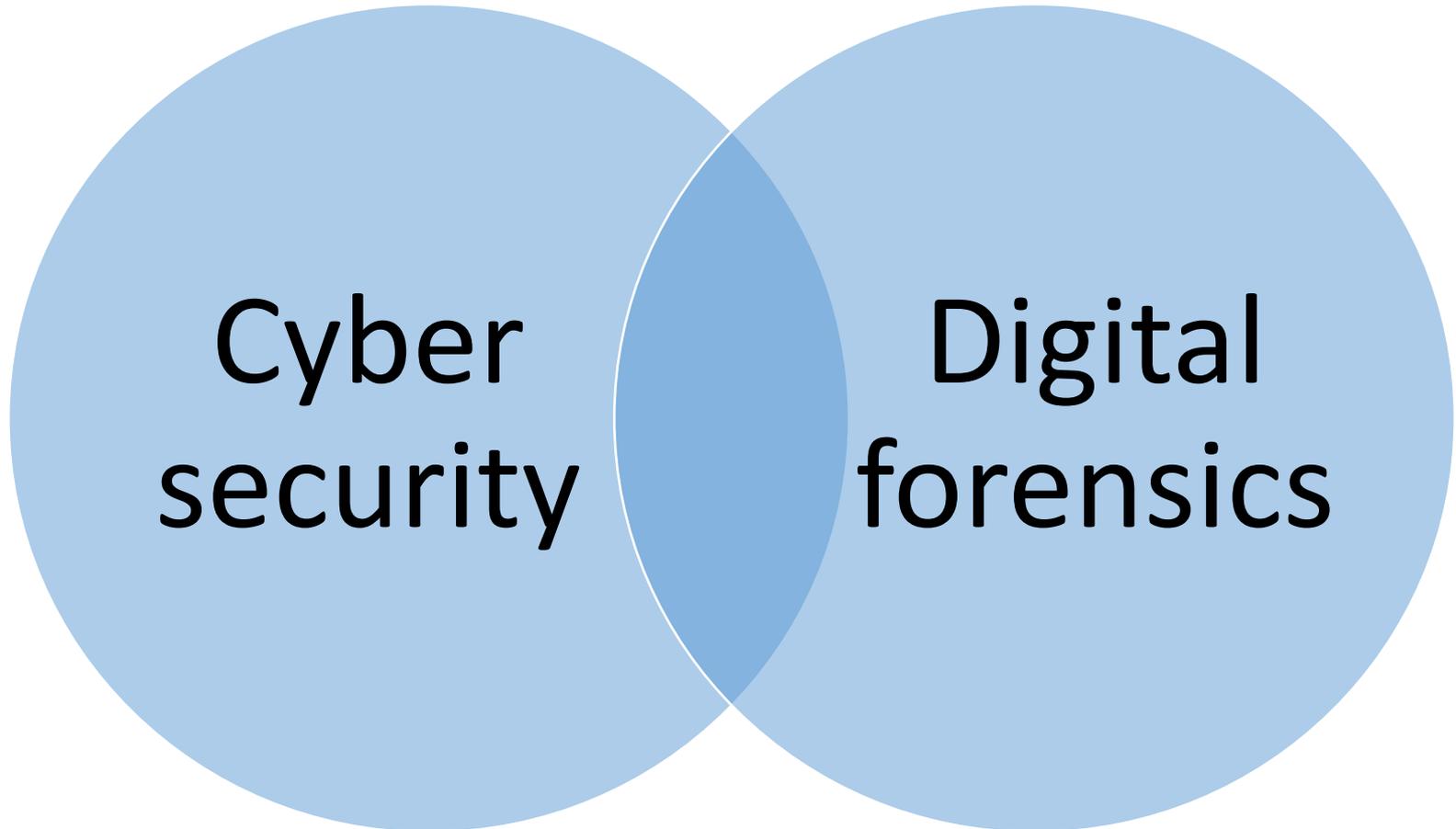
University of Louisville

# Introduction

- Our talk examines aspects of the legal space within which cyber security as a discipline operates.
- We seek to help you:
- Identify and Comply with some of the legal restrictions that can put you crossways with law enforcement in
  - cyber security research,
  - cyber security testing,
  - cyber security implementation,
- Anticipate policy concerns in a cyber security regime, and
- Integrate a traditional criminal justice regime into cyber security as a paradigm for cyber security
  
- This program builds on the excellent CAE Forum presentation of Paula deWitt, Texas A&M, setting context for the essential if abrasive relationship between technology and law.
- *And, yes, this is not meant to be legal advice in any way, form or manner!!!!*

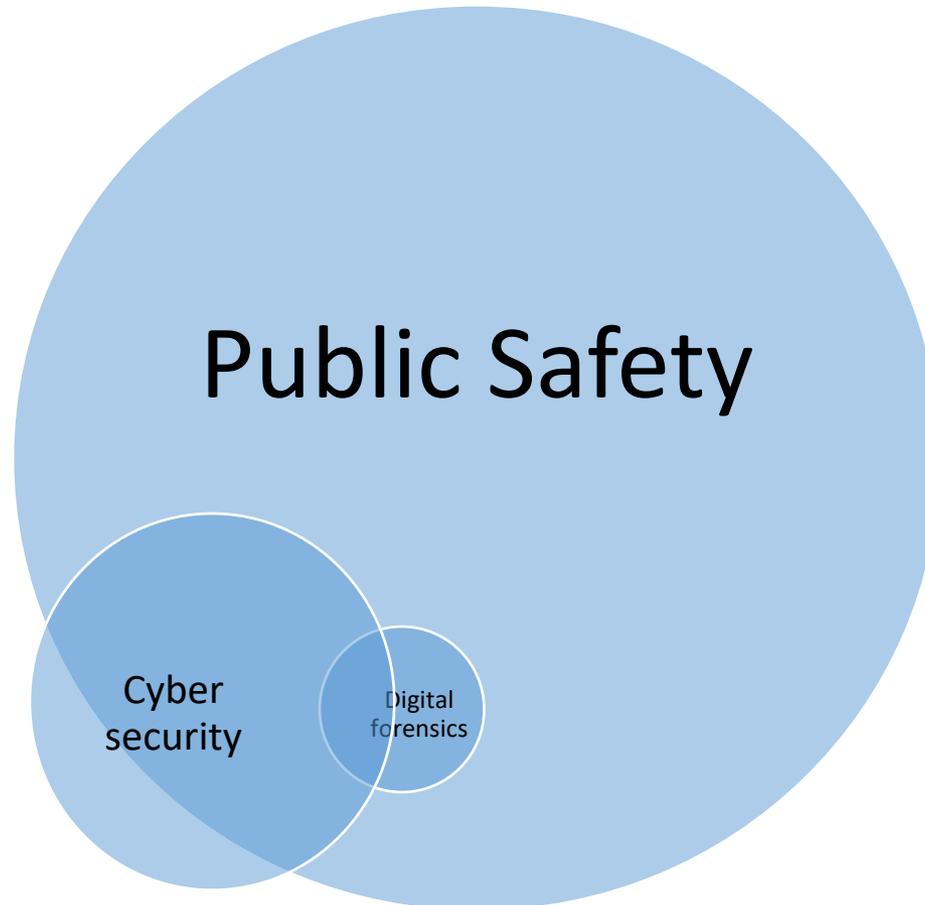
# Context

Back in the day



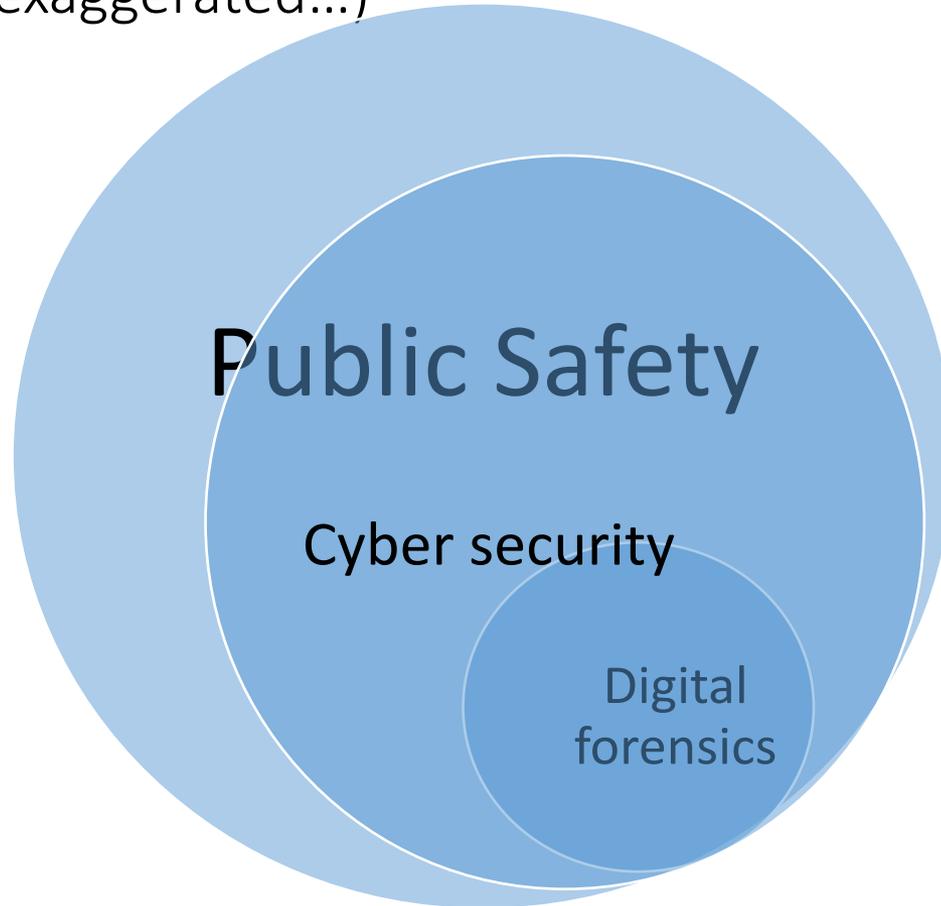
# We submit today

(not to scale...)



And with tomorrow's IOT, Smart City, Ubiquitous networking, Big Data...

(slightly exaggerated...)



# A shout out to our CWE cohort and Ross Anderson's krewe at Cambridge

- ***A Project for Bringing Public Safety Personnel into Cybersecurity Careers***
  - This project aims to increase the pool of cyber security professionals in multiple domains by identifying, recruiting and training practitioners and students in law enforcement and public safety disciplines, including police, probation and parole, military and other public safety areas.
    - Thanks to Ross Anderson's open source cyber security materials and texts at Cambridge University.
    - Thanks to the comments from CWE, Tom Kelly, et al
- We suggest the integration of traditional criminal justice systems and practices into cyber security
  - Experience with the breadth of criminality
  - Experience with grass roots impact of crime
  - Experience with community engagement in reducing the impact of crime

# Cyber Security, Public Security

- Stallings on Computer Security:

- Prevention
- Detection
- Recovery

- Police Foundation (UK)
  - to prevent crime;
  - to pursue and bring to justice those who break the law;
  - to keep the Queen's peace (maintenance of order).
  
- 18 USC 3553-Sentencing (US)
  - Deterrence
  - Incapacitation
  - Rehabilitation

# General issues

- Niedorf, Morris and you
- Duties, laws, ethics
- How do we avoid an “inside” view of Cyber security and cybercrime?

# *Accountability in cyber security research and practice*

- Researchers and practitioners are not immunized from illegal or injurious security activities
- Criminal law liability
  - If it is illegal to possess certain contraband, the fact that it's done for research purposes does not change the criminality
  - If illegal to access a machine without authorization
    - It may be illegal to do so for research
    - it may be illegal to access an attacking machine without authorization
      - What is cyber “self-defense?”
  - When is it legal to intercept electronic communications?
- Civil law liability:
  - Welcome into the wild and woolly world
  - Intentional act leading to injury, negligent acts leading to injury, failure to properly design, failure to properly implement leading to injury, etc. etc. etc.

# Concerns expand...

- State action in violation of the 4<sup>th</sup> Amendment
- Private citizen trespass
- authorized and unauthorized access to a computer
- access to data
- interception of data
- Sui generis and special legal restrictions
- Liability for security failure
- *And so forth, and so on,...*

# Possible concerns

- Who is the reporting authority for cyber security violation
  - Issue of misrepresenting location of offense to invoke a larger jurisdiction.
  - frustration if it's something a particular department cannot handle.
- Is this an issue of education/training?
  - Consider the February CAE forum by Levy and Carlton and their discussion of a Cybersecurity Skills Index (CSI)
- how to document the evidence and build these cases.
  - Many of the larger schemes take place across states lines and can be prosecuted federally.
  - How do we assess the cost of these crimes or losses ?
  - Local law enforcement budget constraints: “smaller” crimes don't meet the threshold  
Corporate compliance-voluntary and with search warrants
- Limitations on search warrants because of intellectual property concerns
- Technical accessibility problems to evidence
- Limitations and liability for data sharing on threats and vulnerabilities?

# Jurisdiction! Defense? Encryption? Privacy?

- Jurisdiction-it belongs to another department
- Jurisdiction-verification
- the different legal frameworks: state level, federal level, international level and then in another country you have another or different set of state, national legal frameworks.
- Honeypots?
- Cyber counter-attacks?
- Encryption?
  - DMCA?
- Mutual Legal Assistants Treaties
- Convention on Cybercrime
- HIPAA
- Juvenile Confidentiality laws
- Privacy Act of 1974

# What do you do in your cyber security research and practice?

- Wait, let me rephrase that: what might you *hypothesize* happens in other people's cyber security research and practice?

- 1

- 2

- 3

- 4

- 5

# Surprise!

## Targets and Contraband in the Network

Contraband	Illegal Conduct
Child pornography	Possession, receipt 18 USC § 2251
Obscene materials	Possession, distribution 18 USC § 1460
Creative content distributed in violation of copyright laws	Copying, distribution 18 USC § 2319
Trade secret information	Distribution, 18 USC § 1831
Technology for Circumvention of copyright protection technologies	Distribution, Digital Millennium Copyright Act
Access devices, including passwords	Possession, distribution 18 USC § 1029

# Surprise!

## "Unauthorized" actions

Five basic types European Convention on Cybercrime as *“Offences against the confidentiality, integrity and availability of computer data and systems”*.

Subjects of regulation world-wide, they are:

- Unauthorized access to computer, (include exceeding authorized access to a computer )
- Unauthorized interception of data ,
- Unauthorized interference with data.
- Unauthorized interference with a system
- Misuse of devices.
  - The Convention looks at intentional conduct “without right.”

# Here at Home

- 18 U.S.C. §§ 2510 et seq. (Wiretap Act/ECPA I) (US)
- 18 U.S.C. §§ 2701, et seq.(ECPA II) (US)
- 18 U.S.C. §§ 3121, et seq. (Pen Register/Trap and Trace) (US)

# An initial evaluative framework

## For network security & forensic investigation

### An initial evaluative framework For network forensic investigation

Category	Nature of Research or Investigative Conduct	1. 1.Yes/No/Don't Know	1. Under what authority?
Unauthorized access to computer	<ol style="list-style-type: none"> <li>Does the conduct access a machine?</li> <li>If so, under what authority or claim of right?</li> </ol>		
Unauthorized interception of data	<ol style="list-style-type: none"> <li>Does the conduct intercept data non-public transmissions of computer data to, from or within a computer system?</li> <li>If so, under what authority or claim of right?</li> </ol>		
Unauthorized interference with data.	<ol style="list-style-type: none"> <li>Does the conduct damage, delete, deteriorate, alter or suppress computer data?</li> <li>If so, under what authority or claim of right?</li> </ol>		
Unauthorized interference with a system	<ol style="list-style-type: none"> <li>Does the conduct seriously hinder the functioning of a computer system by the input, transmittal, damage, deletion, deterioration, alteration or suppression of computer data?</li> <li>If so, under what authority or claim of right?</li> </ol>		
Misuse of devices	<ol style="list-style-type: none"> <li>Does the conduct involve the acquisition, distribution or use of a device or data for illegal access, interception or interference with computers or data?</li> <li>If so, under what authority or claim of right?</li> </ol>		

- 18 U.S.C. § 1030, the Computer Fraud and Abuse Act (US) (“CFAA”)
- Although key elements of this crime, neither "access" nor "authorization" are defined by the federal (US) statute, being left open to jurisprudential (judge) interpretation.

- “Authorized Access” is a *sui generis* definition of computer-related conduct addressing concerns found with the application of traditional concepts of trespass and invasion of privacy .
- Criminal and civil prohibitions on trespass sought to protect against physical intrusion or interference with property, yet prosecutions for trespass via electronic interaction with a computer had to address the lack of physical invasion of the property.
- The idea of “access” as an element was developed for such situations; “authorized access” delineated permitted and unpermitted access to data and system resources.

- One federal court noted “access” as:
  - ... the word "access," in this context, is an active verb: it means "to gain access to," or "to exercise the freedom or ability to make use of something." (citing *Mirriam-Webster's Collegiate Dictionary* 6 (10th ed. 1994)) (internal quotations and alterations omitted).
- Is there explicit authorization to access?
  - User agreements for online services may expressly grant access, though special terms of use may apply
  - States, by statute, may authorize certain types of access to certain groups of people.
  - A court order/search warrant gives the serving officer permission to search and access a computer or system, (exceptions to a warrant an issue?)
  - consent to access authorizes that access, just as any consent to search physical premises obviates the need for a search warrant.
- Is there implicit authorization to access?

# "implicit authorization?"

- One court noted
  - there could be an “implicit” limit on authorized access and
  - expressly declined to adopt the view that that is a “presumption” of open access to Internet information, noting
  - “CFAA, after all, is primarily a statute imposing limits on access and enhancing control by information providers.”
  - “public website provider can easily spell out explicitly what is forbidden and, consonantly, that nothing justifies putting users at the mercy of a highly imprecise, litigation-spawning standard like “reasonable expectations.””, a flawed standard for such situations.

- This leaves little guidance as to what conduct constitutes “access” that becomes subject to a requirement of authorization or right.
- The technical model of an interaction with a machine via a command or messaging may become the default for judging whether or not there has been access.
- This may possibly be mitigated through a calculation of the extent or impact of that access,
- But reliance on that, absent clear, direct, controlling jurisprudence, *may create a risk for a researcher or investigator.*
  - .

# Is this access for network security investigation ?

<b>Service</b>	<b>Category</b>	<b>Nature of Research or Investigative Conduct</b>	<b>1. 1.Yes/ No/ Don't Know</b>	<b>2-Under what authority?</b>
Ping	Unauthorized access to computer	1-Does the conduct access a machine? 2-If so, under what authority or claim of right?	No	
Query	Unauthorized access to computer	1-Does the conduct access a machine? 2-If so, under what authority or claim of right?	No (probably )	
Get	Unauthorized access to computer	1-Does the conduct access a machine? 2-If so, under what authority or claim of right?	Yes	?

# Authorized?

- “Authorized Access”, or access with right, is assumed in the use of these services by placing a machine on the network under the application without blocking the services in some way.
- Each of these services makes greater and greater demand on a target machine for services, responses and data.
- Under an “implicit authority” theory for the “tradition” of the services, such demands may be acceptable.
  - Consider the old Gnutella protocol has been described as “ an open, decentralized group membership and search protocol” [24]; that description implies permissions to participate as part of the group through open access.
  - Would you rely on this?
    - A sliding scale?
    - A prudential scale?

# Case Experiment - Authorized Access via P2P Research Tools

- A P2P research tool may be set to harvest data on query traffic on a network. It harvests query data by placing a machine on the network as a "leaf" that
- transmits to an "ultrapeer" a file ("bit vector") that serves as a routing table with data asserting that it can respond to all queries sent to the ultrapeer.
- All bits in the routing table of the bit vector file are set to claim that all key words for a query match files available on the leaf machine.
- When the ultrapeer passes queries down to the research leaf machine, that research machine harvests the query data but does not respond to it.

- Is transmitting the routing table sufficient to constitute “access?”
  - Such a determination may depend on how the extent of this action is viewed as making use of the system available to the remote users and the tool.
- If access, is it authorized?
  - The use of such a tool may fall outside the expected use and interaction with a node on a P2P network.
  - The routing table file is deceptive as it cannot respond to all queries as asserted; the tool is making a representation for purposes of the data collection, not file sharing.

- Implicit authorization would involve transactions across the network designed to facilitate its use for file and resource transfer.
- As this tool acts only to consume alternative resources for purposes unrelated to the actual use of the network, it raises a question as to whether there is implicit authorization for its operation.
- Yet is there any effort to limit such activity such that authorization is implied?

## How to Remediate

- Kerr suggests new statutes relating to authorized access that expand to specifically address each different type of computer misuse. This would begin with clearly defining “access” as any time a user sends a command to a machine that, in turn, executes the command.
  - Thus Ping = Access
- But he proposes that this broad meaning of access, consistent with the technology, would be matched by a more circumspect definition of access “without authorization” to “access that circumvents restrictions by code.”
  - i.e., a positive obligation to “lock your door.”
- And there should be expanded statutes dealing directly with damage or infringement to systems and data

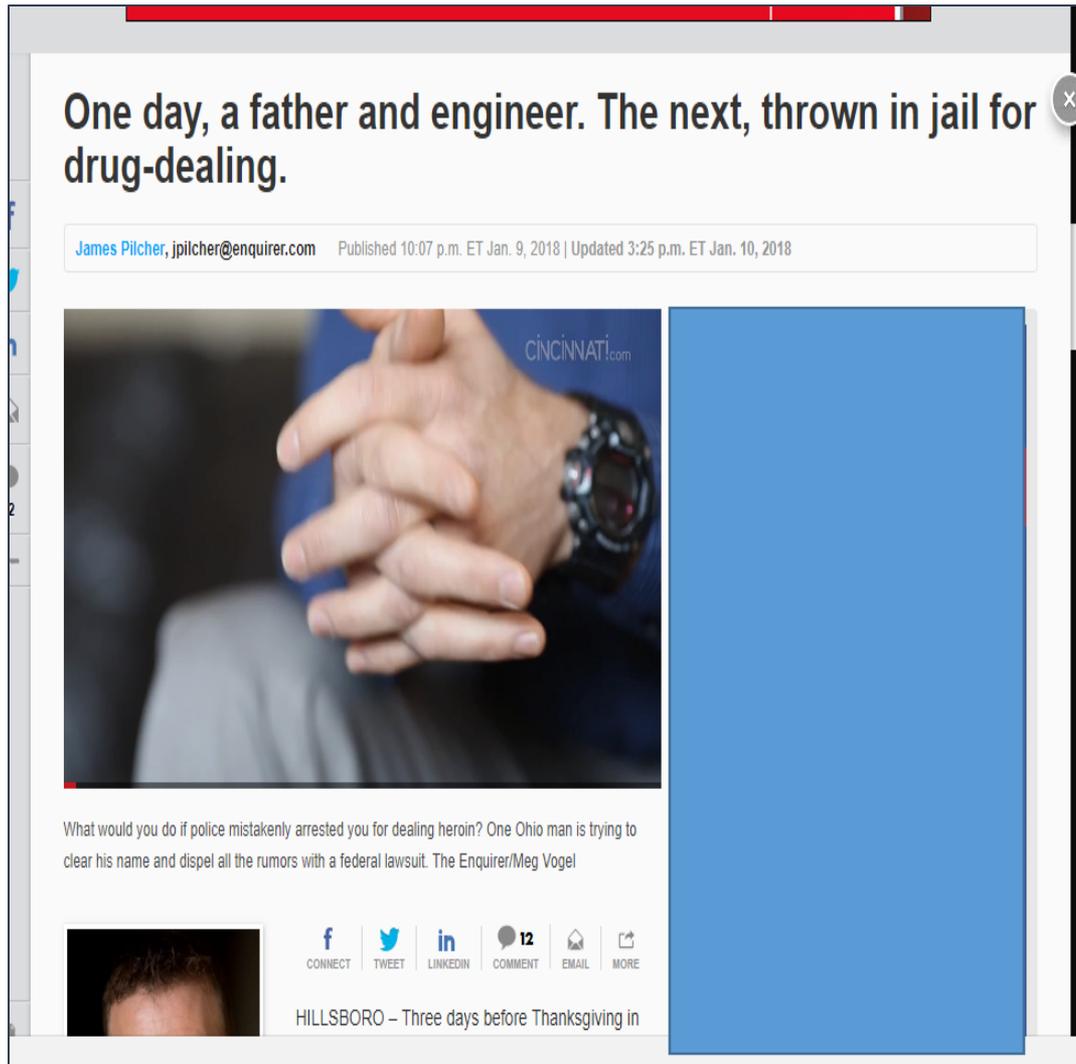
or

- An alternative analysis might match conduct with the level of interaction with a machine, using the OSI model to delineate the hierarchy.
- Analysis of elements of “Entrapment” in online environments
- Analysis of elements of illegal interception of electronic communications
- Analysis of evolving privacy technologies and expectations
- Analysis of possible legislative “safe harbors” for researchers and investigators.

## warning

- Pitfalls remain in analyzing system use over networks, both for state and private investigators and researchers.
- Investigation and research in a simulated testbed environment must lead to real world application.
- Continued analysis of the many legal and ethical implications of investigative techniques is needed for both investigative products and tools that will *later* result from research and also in the *current* research phase in anticipation of testing new tools in the real world.

# Policy Implications and you



**One day, a father and engineer. The next, thrown in jail for drug-dealing.**

James Pilcher, [jpilcher@enquirer.com](mailto:jpilcher@enquirer.com) Published 10:07 p.m. ET Jan. 9, 2018 | Updated 3:25 p.m. ET Jan. 10, 2018



What would you do if police mistakenly arrested you for dealing heroin? One Ohio man is trying to clear his name and dispel all the rumors with a federal lawsuit. The Enquirer/Meg Vogel



[CONNECT](#) [TWEET](#) [LINKEDIN](#) [COMMENT 12](#) [EMAIL](#) [MORE](#)

HILLSBORO – Three days before Thanksgiving in

# More Policy Concerns, and things to come

- *Forensic Data Collection and Analytics-How Growing Data Impact Privacy*
- *United States v. Jones* was the first major US case to present issues of the impact of investigative data technology and analytics. [53] In *Jones* it was the use of GPS tracking devices feeding to a central system. That investigative power drew special comments from both liberal and conservative jurists. Justice Sotomayor, considered a liberal, felt inexpensive computer-mediated geo-spatial tracking could “*alter the relationship between citizen and government in a way that is inimical to democratic society.*” (emphasis added) via GPS data monitoring, aggregation and analysis. It would give the police immense surveillance power that “...evades the ordinary checks that constrain abusive law enforcement practices.”

- *Personal Devices and Their Growing Data Impact Privacy*
- The massive growth in cellular telephone data capacity and diversity led the Supreme Court to put cell phone examination out of bounds without a court order or special circumstances: "modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans 'the privacies of life.'" The Court in *Riley v California* extended protection to new forms of data collection and storage not granted smaller, more static physical media like notebooks precisely because of the new scale, and what it reveals.

- *Anti-Forensics v. Information Security -Forcing Decryption*
  - One man's privacy app is another's sedition tool.
- The first case in New York sought to have Apple crack a phone of a drug dealer, but that judge expressed doubt that Apple could be forced to do so.
- Then the United States government filed a second case to force decryption of an iPhone taken from one of the terrorists involved in mass killings in San Bernardino, California.

- *Transnational Disclosure of Digital Evidence*
- Cloud services and distributed data networks may have global facilities across national boundaries. The United States Department of Justice sought customer emails stored on a Microsoft server outside of the United States. Microsoft refused and the court found no authority to authorize seizure of customer e-mails stored exclusively on foreign servers.
- Despite this, the Department of Justice sought a similar order against Google from a different federal court. Despite support for Google from Microsoft, Amazon, Cisco Systems and Apple, that court ordered Google produce information on servers located outside of the United States
- Now awaiting Supreme Court decision!

- *Third Party Data Collection, Storage And Exchange, and the Analytical Data Personae*
- The Internet of Things and the Smart City will engender huge growth in third-party data collection and storage, which will only expand with the Internet of things, presents new challenges to privacy and personal autonomy.
- The European Union has structured, well-developed regulations with rigorous controls on data collection, storage, transmission and use. Other countries, including the United States, do not.

- 
- *Computational Forensics, Crime and National Security*
- AI forensics analysis, predictive policing and criminal justice decision-making via algorithmic analysis of data sets is growing.
- These technologies-effectively Big Data in the Smart City- are central to the Smart City and fully using the Internet of Things.

# *Bringing Public Safety Personnel into Cybersecurity Careers*

- increase the pool of cyber security professionals in multiple domains by identifying, recruiting and training practitioners and students in law enforcement and public safety disciplines, including police, probation and parole, military and other public safety areas.
- We suggest the integration of traditional criminal justice systems and practices into cyber security
  - Experience with the breadth of criminality
  - Experience with grass roots impact of crime
  - Experience with community engagement in reducing the impact of crime
- Local law enforcement is close to the ground zero of much of cyber criminality and its victims
  - Can respond
  - Can advise
  - Can arrest

# Conclusion

- It is essential that security research that seeks to address misconduct in the use of devices and networks, whether of security compromises or other illegal activity, take into account possible legal restrictions on such activity.
  - Good intentions are simply not enough.
  - Failure to address legal limitations may both compromise the evidentiary value of research techniques developed as well as expose researchers to legal liability and damage to reputation.
- *Thank you, colleagues*