SANS @ CYBERWEEK

Cyberlaw Today

Ben Wright

@benjaminwright

Cyber Law

Benjamin Wright, Texas Attorney

SANS Institute Instructor for Course titled

LEG523 “Law of Data Security and Investigations”

benjaminwright.us

I Welcome Comments and Questions as We Go Along

Background

- I aim to inspire rather than provide a cookbook of solutions
- I’m humble about these topics
- This is not legal advice for any given situation. If you need legal advice, you should consult your own lawyer
-

Investigations

The Power of Self-Serving Language

- Self-serving language can be used in policies, contracts, terms of use
- Tilts legal outcome in an ambiguous world
- Labels of ownership or boundaries are influential

Warning! No Trespassing.
This system is monitored.

U.S. v. Heckenkamp

- University of Wisconsin SysAdmin is suspicious
- Hacks into student's PC
- Violate 4th Amendment (privacy)?
- 9th Circuit Court of Appeals: No, because student consented to the hack in network terms of service

Wise Investigators Read Terms of Service

Terms Can Forbid Evidence Collection

- Patent owner agrees to terms at a dating website that say, "personal use" only
- Owner makes screenshots of website suggesting site violates patent
- Court: Terms can forbid the collection of evidence and making of records; however, these terms simply do not say that. Evidence admitted
- *TRUEBEGINNINGS, LLC v. Spark Network Services*, 631 F. Supp. 2d 849 - Dist. Court, ND Texas 2009

WhatsApp Terms of Service

- NSO Group works for governments, allegedly making spyware to infect phones of investigative targets via WhatsApp
- Allegedly NSO runs a platform that facilitates infection in the WhatsApp platform
- Facebook (owner of WhatsApp) sued NSO for violating WhatsApp terms of service
- Lesson: official investigators should read the terms of websites/mobile apps

Lessons from Coalfire-Iowa Penetration Test Disaster

Setting the Stage

- Lessons Apply Beyond Pen Testing
- This case: Client hires contractors to do dicey work
- Communications and documentation are weak and confusing
- Client and contractors both suffer
- Same could happen in many DFIR contexts

The Plot

- Iowa State Court Administration hires Coalfire to pen test
- Scope broadly includes physical entry into county courthouses
- 2 pen testers break into Dallas County Courthouse at midnight
- Sheriff arrests
- Prosecutor indicts

Poor Judgment & Communication

- Client's representatives were IT folks
- They had not deeply thought about the legal and political implications of testing a county courthouse
- Pen testers were not keeping client fully informed

Generic Lesson

- Documents need to be carefully written
- The “get of jail free card” spoke of social engineering, not physical probing after hours
- Card prohibited “Force-open doors” … does that prohibit lock-picking?
- Documents were boilerplate jumble
- Phone number for one contact was wrong

How to Achieve Compliance

Promote Compliance – With Everything

- Many laws, regulations, standards
- They demand much in a changing world
- Three measures I like:
  - Appointment of an accountable officer
  - Periodic certificate signed by officer
  - Emphasis on “professional teamwork”

Models for Periodic Certificates

- Federal Information Security Management Act (FISMA)
- New York Department of Financial Services Cybersecurity Regulations
- Sarbanes-Oxley

Example Certification

- For use world-wide
- "To the best of my knowledge, Acme Org. applies professional teamwork to cybersecurity. Signed -CISO of Acme Corp."

Why “Professional Teamwork”?

- Hospitals held to a “professional teamwork” standard
- Neither hospitals nor cyber defenders should be expected to be perfect
- No particular cyber defender is a professional like a licensed doctor or accountant
- A qualified, well-resourced cyber security team as a whole can provide a professional grade of attention to problems

Generic Problem in Cyber Law

- How to tell the full and candid truth?
- Technical reality is complex
- How to summarize the truth in a certificate or response to a questionnaire?
- Much legal risk boils down to telling the truth
- It can take years for the real or full truth to come out

How to Take Responsibility for Security

- Lesson from CISO at a US Department of Defense agency
- Certificate required by Federal Information Security Management Act (FISMA)
- How to be accountable
- How to tell the truth
- Sign a certificate of compliance, but include with it a memo describing known caveats or shortfalls

Use the Legal System

File a Lawsuit

- Microsoft vs Waledac botnet – seize domain names
- Southwire vs Ransomware
  - Order from Irish court
  - Followed with publicity at onesouthwire.com

- Big, generic idea: Seek help from an authority

China Intel Officer Arrested in Belgium

- Extradited to US on charges of stealing trade secrets from GE Aviation, a US firm
- GE Aviation credits is partnership with FBI
- Pete Williams, “Chinese intelligence officer charged with conspiring to steal secrets from U.S. firm,” October 10, 2018 nbcnews.com

Act “Proportionate” to the Situation

- “Proportionality” is widely accepted standard in difficult situations like self-defense
- Document you are acting proportionate to
  - Vulnerabilities
  - Damage
  - Storage/destruction of records

GDPR Privacy: Balance and Proportionality

- Privacy is right to be left alone; that includes right not to be victimized by terrorists
- Therefore, Europol is justified to use Big Data to find terrorists, even though Big Data might inconvenience the privacy of terrorists
- EU privacy states absolute principles, but the principles are subject to balance and proportionality
- “The BIG DATA Challenge: Impact and opportunity of large quantities of information under the Europol Regulation,” Computer Law & Security Review, Volume 33, Issue 3, June 2017, pages 298–308. www.sciencedirect.com/science/article/pii/S0267364917300699.

Comments and Questions

Visit Ben's Profile Page for His Additional Resources

sans.org/profiles/benjamin-wright/

@benjaminwright

ADDITIONAL CONTRIBUTIONS BY BENJAMIN WRIGHT

WEBCASTS

Coalfire Penetration Testers Charged with Criminal Trespass, May 2020

The Global Privacy Law Imperative, July 2019

LabMD: The Phony Data Breach, June 2018

Sensitive Data Everywhere: Results of SANS 2017 Data Protection Survey, Sept 2017

Complying with Data Protection Law in a Changing World, June 2017

Lingering Exploits Related to WannaCry Ransomware?, May 2017

Latest on WannaCry Ransomware, May 2017

Complying with the General Data Protection Regulation: A Guide for Security Practitioners, March 2017

PUBLICATIONS

Blog: https://www.linkedin.com/in/benjamin-l-wright/

Book: The Law of Electronic Commerce