General note

No mobile please

Question?
Griffith & Kohlmeier

Benjamin E. Griffith
- Griffith Law Firm
- IMLA International Committee
- ABA Board of Governors

Sven Kohlmeier
- Kohlmeier Law Firm
- Attorney at Law, professional lawyer specializing in IT law,
  Mediator
- Member of Berlin House of Representatives
Introduction

- How do you feel in the time of global internet communication?

- Where better live to protect against government surveillance – US or Europe?
Question to the auditorium

- Who is using unencrypted emails?
- What do you know about cyber theft?
- Who is using a cloud solution to store private or business-based data?
What we are talking about

cloud using
attacks to smart city infrastructure
antiquated hard- and software
government surveillance
cybertheft
manipulation of public opinion
open data portals
attacks on government IT-structure
Introduction: Scope of the Problem
Government Surveillance – National services are watching you

- Does the NSA collect any type of data at all on millions, or hundred millions, of Americans?

- „....not wittingly....“

  (James Clapper)
Privacy interest in a global surveillance world

- Is there still privacy safeguard in our electronic communication e.g. emails, chats, whatsapp app and similar?
Government Surveillance

United States Court of Appeals
FOR THE SECOND CIRCUIT

August Term, 2015


Docket No. 14-2985

In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation

Microsoft Corporation,

   Appellant,

   v.   

United States of America,
Government Surveillance

14.07.2016: Docket No.14-2985
Court of Appeal, New York

“Accordingly, the SCA does not authorize a U.S. Court to issue and enforce an SCA warrant against United States based service provider for the contents of a customer’s electronic communications stored on servers located outside the United States.”
Government Surveillance

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

In re Search Warrant No. 16-960-M-01 to Google
Misc. No. 16-960-M-01

In re Search Warrant No. 16-1061-M to Google
Misc. No. 16-1061-M

MEMORANDUM OF DECISION

THOMAS J. RUETER
United States Magistrate Judge

February 3, 2017

In August, 2016, this court issued two search warrants, pursuant to section 2703 of the Stored Communications Act, 18 U.S.C. §§ 2701 et seq. (“SCA” or “Act”), which required Google Inc. (“Google”) to disclose to agents of the Federal Bureau of Investigation (“FBI”) certain electronic data held in the accounts of targets in two separate criminal investigations.

Government Surveillance

- 03.02.2017: U.S. District Court, Philadelphia, HONORABLE THOMAS J. RUETER

- “Electronically transferring data from a server in a foreign country to Google’s data center in California does not amount to a “seizure” because there is no meaningful full interference with the account holder’s possessory interest in the user data.” (page 20)

- Conclusion: “For all the above reasons, the court will grant the Government’s motions to compel Google to comply with search warrants.”
State of Cybersecurity in Local, State & Federal Government

- Infrastructure is becoming one of the ripest targets for cyber attackers.
Reasonable Cybersecurity Actions Based on Threat Profile

- What is the local government entity’s risk appetite?
Interrelated Cybersecurity Issues
Projected Costs for Cybersecurity Protection

- Advances in Technological Innovation vs. New Opportunities for Exploitation
A Quick Look at the Numbers

- BP claimed to have suffered 50,000 attempted cyber intrusions per day.
- The Pentagon reported 10 million cyber intrusion attempts a day.
- The U.S. Energy Department’s National Nuclear Security Administration recorded 10 million hacks a day.
- The United Kingdom reported 120,000 cyber incidents per day.
- The State of Utah claimed to have 20 million attempts per day, up from 1 million per day two years before.
Attack against German Telekom Internet routers

- Strongest DDos-attack with Mihai-malware
Attack on Cellebrite with theft of 900 GB of data
Cyber attacks on the German Armed Forces
Cyber Attack on the German Bundestag
Segate’s $55 Million ATM Cashouts
Europol Cross-Border Cooperation

- International engagement on cybersecurity is essential, and Europol’s efforts proved it.
Ramnit: Public-Private Collaboration to Enhance Cybersecurity
Financial Malware
Chelan County, Washington v. Bank of America Corporation
Iranian Cyber Attacks Targeting New York Dam
A possible motivation for the Iranian-led cyber-attack on a New York dam in 2013 may lie in events several years before surrounding the Stuxnet virus.
Spearphishing & Disruption of Attack Delivery

1. A hacker targets a company. Using social networks or other internet data, he finds employees with access to company data/systems.
2. Following the social trail, he identifies other people the employee may know.
3. A fake but recognizable email address is created to impersonate a colleague or boss.
4. A personalized email is sent to the employee from the fake address with a link or attachment.
5. The email passes the spam filter and arrives at the employee’s inbox.
6. The email is opened because they ‘know’ the sender.
7. A link is clicked or attachment opened.
8a. Opened website causes credentials to be stolen/malware to be installed.
8b. Opened attachment causes malware to infect the computer/smartphone/network.
9. The hacker uses the backdoor to steal information.

ANATOMY OF A SPEAR PHISHING ATTACK
Multi-Stage Attacks by State-Sponsored Actors

From: Coca-Cola Company <customers@coca cola.us>
Date: Mon, 10 Jan 2011 04:39:54 -0600
Subject: Happy New Year

Dear [Name],

You have been selected to participate in a public opinion poll conducted by Coca-Cola, a non-partisan polling organization.

The poll is about current events at the national level and your views about them. It is short and should take you only 5-7 minutes to complete. All of your answers will be kept strictly confidential and will be used only for legitimate research purposes.

To take the poll, click on this link:
www.CocaCola.co.uk/Survey_Pool/150Dollar5-7min/Survey.html

Each person taking the poll will win $150

Thank you for your participation!

Sincerely,
Survey Manager

© 2010 The Coca-Cola Company, all rights reserved. Coca-Cola and the Coca-Cola contour bottle are registered trademarks of The Coca-Cola Company.
Aramco attack
Zeus Virus and Masquerading

- Stealing Confidential Information from Compromised Systems
- Wide Array of Targets in and Outside Government
- Inability to Remove All Versions from Operating Systems
Replay Masquerades

Darth

Capture message from Bob to Alice; later replay message to Alice

Internet or other comms facility

Bob

Alice
Protection Methodology

- Cat and Mouse
- Attack Vectors
The Cybersecurity Information Sharing Act (CISA)

1. Allows companies to share nearly ANY type of information with the government, including significant amounts of personal information.
2. NSA and FBI automatically get all shared information and can use it for any number of reasons.
3. Protects companies from being sued for sharing your personal information.
4. Allows "hack backs" that could damage 3rd party networks, and also creates a vast new exemption to transparency laws.
Immunity from Consumer Lawsuits

- One of CISA’s key features is that it enables private entities, non-federal government agencies, state, tribal and local governments who have been victims of cyber threats to share information with any federal entity and with each other.
Governmental Cybersecurity Clearing Houses and Measures at Federal and State Level

- The new clearinghouse created by CISA focuses on cyber threats.
New Jersey League of Municipalities Cybersecurity Awareness Efforts

- Awareness at the Municipal Level
- Education and Outreach at N.J. Local Government Level
- Franklin Township’s Fight Against Cyber Threats
Municipal Targets of Cyber Threats

Cyberattacks are mostly targeting...

- **36%** of government
- **33%** of individuals
- **39%** of corporate world
- **46%** of 45 to 54 years old

*Base: 513 online respondents representative of the general US population. Interviews conducted between November 23rd and November 25th, 2016*

reportlinker.com/insight
## Better Security with Slot Machines than Computer Voting Systems?

A look at how Las Vegas slots and electronic voting machines compare:

<table>
<thead>
<tr>
<th>LAS VEGAS SLOTS</th>
<th>ELECTRONIC VOTING MACHINES</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Software</strong></td>
<td>State of Nevada has access to all software. Illegal to use software that is not on file.</td>
</tr>
<tr>
<td><strong>Spot-Checking</strong></td>
<td>State gaming inspectors show up unannounced at casinos to compare computer chips with those on file. If there is a discrepancy, the machine is shut down and investigated.</td>
</tr>
<tr>
<td><strong>Background Security</strong></td>
<td>Manufacturers subjected to background checks. Employees are investigated for criminal records.</td>
</tr>
<tr>
<td><strong>Equipment Certification</strong></td>
<td>By a public agency at arm’s length from manufacturers. Public questions invited.</td>
</tr>
<tr>
<td><strong>Handling Suspects</strong></td>
<td>Casino must contact the Gaming Control Board, which has investigators on call round the clock. They can open up machines to inspect internal mechanisms and records of recent gambling outcomes.</td>
</tr>
</tbody>
</table>
DDoS: Distributed Denial of Service

- Purchase of DDoS Service on the Dark Web
- Approaches to Prevent DDoS Attacks
Grass Roots Approach to Cyber Security

- Recognizing the Problem
- Coordinated Governance via a Cyber-security Governance Committee
- Engaging Stakeholders
Smart Cities and Protection of Citizens from Cyberattacks
Post-Ferguson DDoS Attack

Following the fatal shooting of Michael Brown by a Ferguson, MO police officer on August 9, 2014, the City of Ferguson found itself at the epicenter of worldwide attention, including that of hackers with a sociopolitical agenda.
Understanding Hactivists’ Motivation, Means, and Opportunity

![Anonymous Logo]

**Anonymous**: Expect Us
Encrypted iPhones and the Battle for Encrypted Data Access

- Device management feature lacking
- Going Dark
- Encryption Backdoors
- Alternative Avenues to Encryption: Cloud Backup
Albuquerque P.D. Going Dark
Essential Preparation and Planning

- Basic measures local governments can take
- Developing Nations’ Reach for Cyberspying Capabilities
Cyber Sanctions
FinFisher

- FinFisher Gamma Group in Munich has developed and produced a sophisticated, user-friendly spyware that is sold exclusively to government agencies and police forces.
IT-Department: How the Berlin Authorities Protect Themselves Against Cyber Attacks

One attack per week is launched as part of secret service activities
IT-Department-Service Berlin:

- eGovernment-Law regulate:
  1. All authorities of Berlin must use IT-Department-Service Berlin
IT-Department-Service Berlin:

- eGovernment-Law regulate:
  2. All authorities of Berlin must create and implement IT security concepts
IT-Department-Service Berlin:

- eGovernment-Law regulate:
  3. All authorities of Berlin supposed to have one IT security officer
IT-Department-Service Berlin:

- eGovernment-Law regulate:
- 4. Computer Emergency Response Teams (CERT) collects and processes IT security incidents
IT-Department-Service Berlin:

- eGovernment-Law regulate:
- 5. Encrypted communication between authorities and citizien/users
What City Officials Need to Know About Cybersecurity

- Cybersecurity Awareness Training
Cryptolocker

Your personal files are encrypted!

Your important files *encryption* produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a unique public key *RSA 2048* generated for this computer. To decrypt files you need to obtain the *private key*.

The single copy of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will destroy the key after a time specified in this window. After that, nobody and never will be able to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay 300 USD / 300 EUR / similar amount in another currency.

Click «Next» to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.
Cybersecurity Awareness Programs
End-User Education

- Security Audits, Penetration Tests and Monitoring
- Security Information and Event Management (SIEM) Tools
- Continuity of Operations Plans
Questions for Local Government Leaders to Consider

1. Questions the human resources department on whether it can help support a security awareness-training program.

2. Give support for new hardware, software, or services.
Questions for Local Government Leaders to Consider

3. Perform assessments, within the limits of funding, at the executive management level regarding the amount of risk the local government is willing to mitigate or simply accept.

4. Make the backup and recovery plan a good as the government can afford, since a cyber attacker with the time and desire will gain access one way or another.
Basic Cybersecurity Best Practices

1. Effective password management policies, using best practices for password management

2. Conductor regular penetration tests and vulnerability scans of infrastructure.

3. Least privilege user access (LUA). Harden client devices by deploying multilayered firewall protections
5. Mobile device management program, requiring authentication to unlock a device, locking out a device after five failed attempts, using encrypted data communications/storage, and enabling the remote wiping of devices if a mobile device is lost or stolen.

6. Continuous monitoring in real-time the security of the organization’s infrastructure.
Basic Cybersecurity Best Practices

7. Deploy web application firewalls to detect/prevent common web attacks.

8. Permit only authorized wireless devices to connect to the network.

9. Implement Always On Secure Socket Layer (AOSSL) for all servers requiring log in authentication and data collection.
Basic Cybersecurity Best Practices

10. Review server certificates for vulnerabilities and risks of domains being hijacked.

11. Develop, test, and continually refine a data breach response plan.
Best Practices for Municipalities

- Encryption
- Control over Administrative Functions
- Strong Password
- Cybersecurity Staff
- Shared Service Agreements
- Cybersecurity Policies
ICS-CERT: Cybersecurity Measures for Water and Wastewater Industry

- Are there feasible, established, vetted, and available best practices and training measures for reducing the risk of such attacks, mitigating the vulnerabilities, and improving the resiliency of such systems?
Best Practice Plus:

*protect your personal and business data and observe the attorney-client privilege*

- Protection of Internet-router/internet-devices
- Internet use
- Internet usage via the TOR network and VPN-Connection
- Internet usage with LiveCD
Best Practices Plus

- Internet usage with a different IP address
- Email usage
- Cloud services
- Network technology and computer repair works by external service providers
Many valuable state and local government cyber-exercises have taken place across the United States, demonstrating successful public-private partnerships and substantive sharing of information and cyber technology.
ABA House of Delegates
Resolution 108
Conclusion
Thanks for your attention