

The Death of Privacy

A Tale of Collusion and Corruption



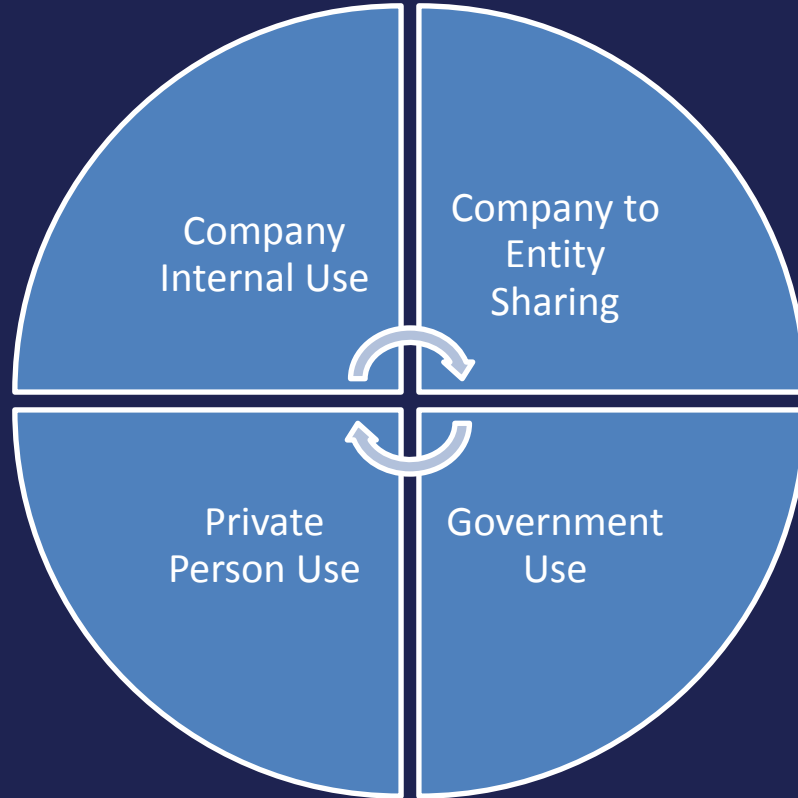


Bummer!

Enlighten - Empower - Entertain

Accessed – Absconded – Abused

Breach of Privacy Opportunities





Company
Internal Use

“defined by the internal practices a company or business entity employs when managing your personal information”

“defined as either a Company
to Third Party voluntary or
involuntary sharing
relationship”



Company to
Entity
Sharing

"defined as information the
Government collects about
you with or without your
permission"



Government
Use



Private
Person Use

"defined as information a
stranger collects about you
again, with or without your
permission"

Here are some recent headlines ...

F.T.C. Fines Google \$22.5 Million for Safari Privacy Violations: The Federal Trade Commission fined Google \$22.5 million on Thursday to settle charges that it had bypassed privacy settings in Apple's Safari browser to be able to track users of the browser and show them advertisements, and violated an earlier privacy settlement with the agency.

Verizon has been slapped with a **\$7.4 million fine** by the U.S. Federal Communications Commission for failing to give 2 million customers the choice of opting out of the company's marketing campaigns. It is the largest fine the FCC has ever imposed for a privacy violation of phone customers' personal information.

A recent and much larger
revelation ...

The NSA is Spying on Millions of Americans: Today, the Guardian newspaper confirmed what many have long claimed: the NSA is conducting widespread, untargeted, domestic surveillance on millions of Americans. This revelation should end, once and for all, the government's long-discredited secrecy claims about its dragnet domestic surveillance programs. It should spur Congress and the American people to make the President finally tell the truth about the government's spying on innocent Americans.

Think this is just an Edward Snowden era issue? This timeline actually begins back in 1952. (Source) <https://www.eff.org/nsa-spying/timeline>

Privacy is the number one concern of Internet users; it is also the top reason why non-users still avoid the Internet.

Survey after survey indicates mounting concern. (Source) The Center for Democracy and Technology

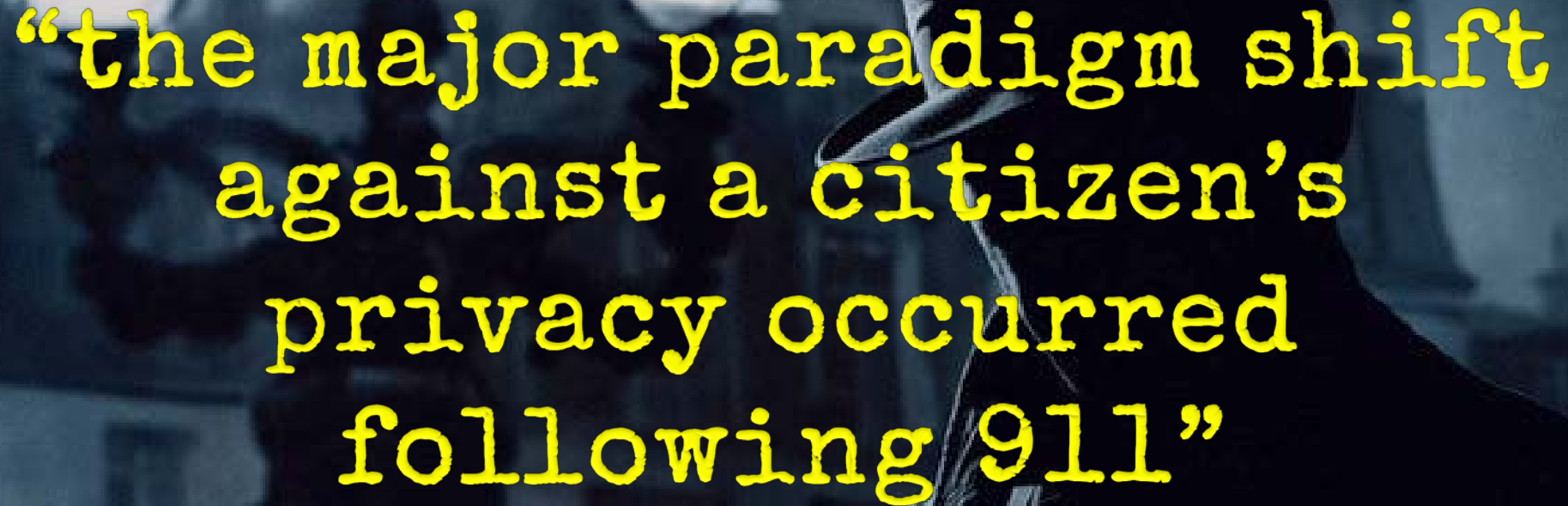


“isolate yourself from the world around you”

Mandate - Monitor - Magistrate

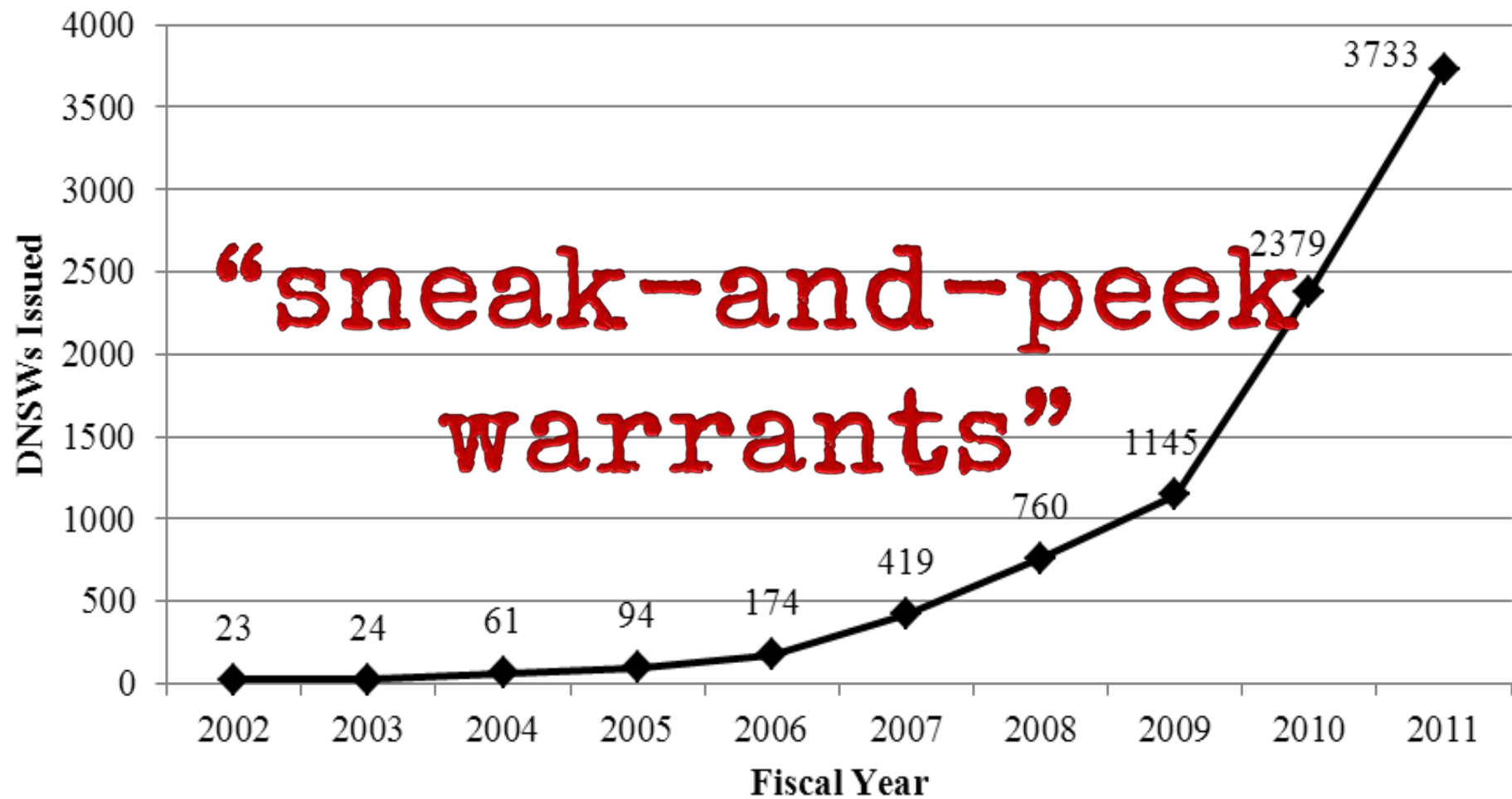
The background of the image is a dark grey grid filled with hundreds of small, colorful icons. These icons represent various digital services, social media platforms, and applications, such as Facebook, Twitter, YouTube, and various email clients. The icons are arranged in a regular pattern, creating a textured, mosaic-like effect.

“the right to privacy
and freedom from
arbitrary invasions”



“the major paradigm shift
against a citizen’s
privacy occurred
following 911”

Fig. 1: Delayed Notice Search Warrants Issued



A close-up photograph of a man's face, specifically his mouth and nose. His mouth is completely covered by a piece of grey duct tape, symbolizing being gagged or silenced. He is wearing a blue and white vertically striped dress shirt and a dark brown necktie. The background is plain white.

“National Security Letters
carry gag orders”

Geez Michael, do you have
anything positive for us?



The Good News!

Common Denominators?

- Fully 75% say their organizations are as or more vulnerable to malicious code attacks and security breaches compared with a year ago. And in the face of a crushing skills shortage, 40% subsist on no more than 5% of the IT budget.
- "Managing the complexity of security" reclaimed the No. 1 spot among 10 challenges facing the respondents to our security survey, all from organizations with 100 or more employees.
- 58% see an infected personal device connecting to the corporate network as a top endpoint security concern, making it the No. 1 response, ahead of phishing and lost devices.
- 56% say cyber-criminals pose the greatest threat to their organizations this year, the top answer, ahead of authorized users and employees at 49%.
- 23% have experienced a security breach or espionage in the past year.

(Source) InformationWeek 2014 Strategic Security Survey



“clearly there is responsibilities
everywhere”



**THE INTERNET
OF
THINGS**

“my whole life is on
my phone”

Structured data
Petabytes
Data analysis
Unstructured content
DATA
Volume
Useful
Meta
Analytics
Smart content
Decision making
database
Text analytics
Concept extraction
Semantic Net
Structured
People driven

- Use encryption!
- Don't reveal personal details to strangers or just-met "friends".
- Beware sites that offer some sort of reward or prize in exchange for your contact information or other personal details.
- Remember that YOU decide what information about yourself to reveal, when, why, and to whom.
- Use a password manager.
- Read the access privileges for apps carefully, and make good choices.
- Keep your work and personal presences separate.
- **Be an activist!**

- Use encryption!
- Don't reveal personal details to strangers or just-met "friends".
- Beware sites that offer some sort of reward or prize in exchange for your contact information or other personal details.
- Remember that YOU decide what information about yourself to reveal, when, why, and to whom.
- Use a password manager.
- Read the access privileges for apps carefully, and make good choices.
- Keep your work and personal presences separate.
- Keep a "clean" e-mail address.
- Realize you may be monitored at work, avoid sending highly personal e-mail to mailing lists, and keep sensitive files on your home computer.
- Do not reply to spammers, for any reason.
- Examine privacy policies and seals.
- Disable GPS and Wi-Fi on your mobile device until you need them.
- Read the access privileges for apps carefully, and make good choices.
- Guard your date of birth and telephone number.
- Make yourself more difficult to find on social media.
- **Be an activist!**

Governance - Technology - Vigilance



The Security Trifecta

On the Horizon?

- **Data Security and Breach Notification Act of 2014**
- **Safe and Secure Federal Websites Act of 2013**
- **The Florida Information Protection Act of 2014**
- **PCI DSS V3**
- **Safe Harbor**
- **Cyber Essentials**



Thank you!



Michael D. Peters

eJD, MBA, C|CISO, QSA, CISSP,
CRISC, CMBA, CISM, CCE, SCPA,
ISSA Hall of Fame

CEO Lazarus Alliance, LLC

762-822-4174

Michael.Peters@LazarusAlliance.com



Visit LazarusAlliance.com for:

- ✓ PCI DSS and PCI SAQ
- ✓ FedRAMP, FISMA and NIST
- ✓ HIPAA, HITRUST, NIST 800-66 and Meaningful Use
- ✓ SSAE 16 (SOC 1), AT 101 (SOC 2) and SysTrust / WebTrust (SOC 3)
- ✓ Cyber Essentials Plus
- ✓ ISO 27001, 27002 and 27005
- ✓ Safe Harbor
- ✓ SHOP CERTIFIED
- ✓ NERC CIP
- ✓ IT Audit Machine®
- ✓ Vulnerability and Penetration Assessments
- ✓ Your Personal CXO®
- ✓ Policy Machine® and IT Governance
- ✓ IT Risk Assessment
- ✓ Cyberspace Litigation Support
- ✓ Holistic Operational Readiness Security Evaluation (HORSE) Wiki®
- ✓ Expert Witness