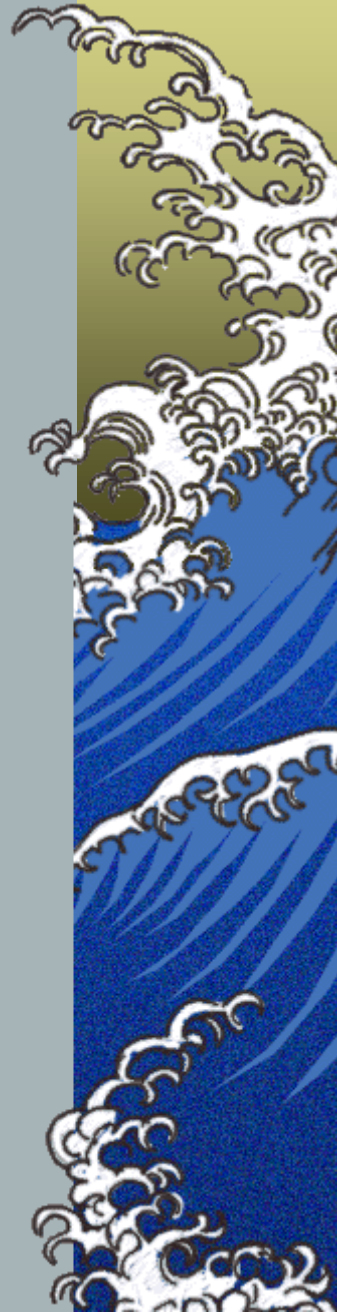




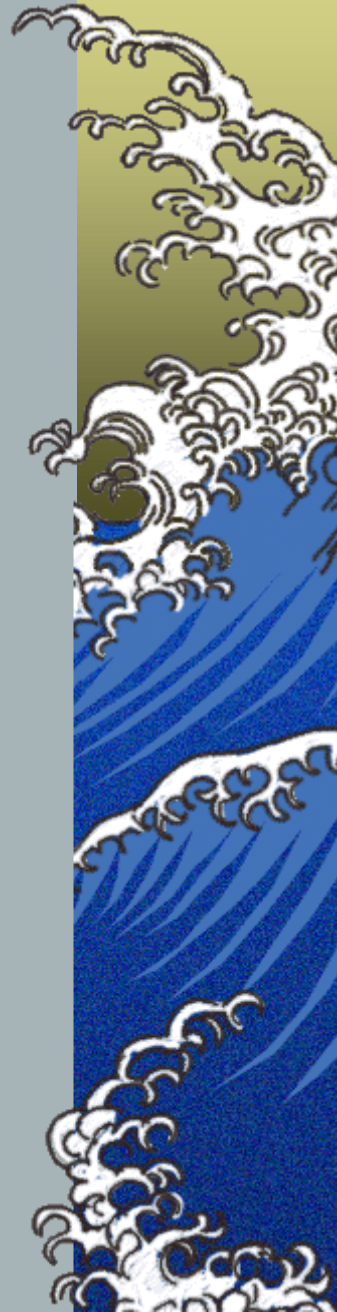
© *The USA PATRIOT Act and You: A Legal Update*

- ▲ *Jennifer Stisa Granick, Esq.*
 - ▲ *Stanford Law School*
- ▲ *Center for Internet & Society*
 - ▲ *559 Nathan Abbott Way*
 - ▲ *Stanford, CA 94305*
- ▲ *650-724-0014*
- ▲ *jennifer@granick.com*



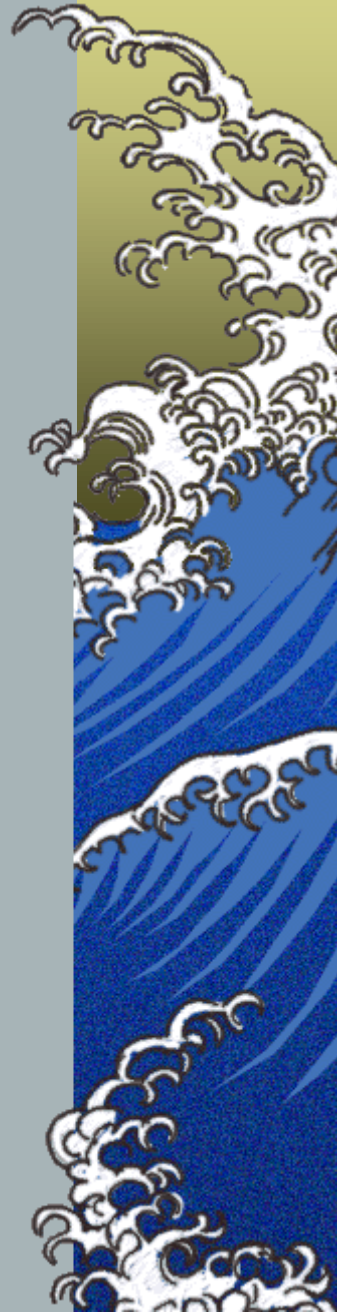
What Can I Do?

- **Lobbying Works: Call or Write Your Congressperson**
- **Get Educated**
 - **American Civil Liberties Union:**
<http://www.aclu.org/issues/cyber/hmcl.html>
 - **Electronic Frontier Foundation:**
www.eff.org/Privacy/Surveillance/Terrorism_militias/20011031_eff_usa_patriot_analysis.html
 - **Center For Democracy and Technology:** www.cdt.org
 - **Electronic Privacy Information Center:** www.epic.org



What is the USAPA?

- ▶ *Drafted Before September 11*
- ▶ *Rapidly Passed Following 9/11*
- ▶ *Increases Gov't Surveillance Powers*
- ▶ *Foreign Intelligence and L.E. Can Share Information*
- ▶ *Defines More Terrorist Offenses, Including Some "Hacking"*



Government Surveillance

- ▶ *Increases Ability of Law Enforcement to Obtain Information*
- ▶ *Problem is Lack of Judicial Oversight and Review*



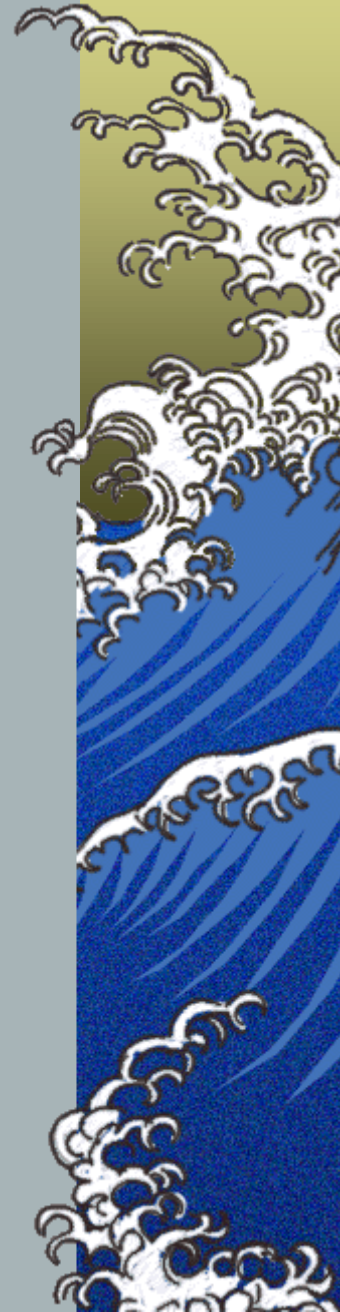
Changes to L.E. Power

▲ *BEFORE*

- *Subscriber Info available with Subpoena.*
 - *IPs, payment info, including CC and bank acc't numbers available with 2703(d) order*
- *Email headers: arguably content data (Title III Warrant)*

▲ *AFTER*

- *Now includes IP, information re: payments, session times and durations. Sec 210, 211*
- *Pen Register/Trap and Trace Order (Issue, subject line)*



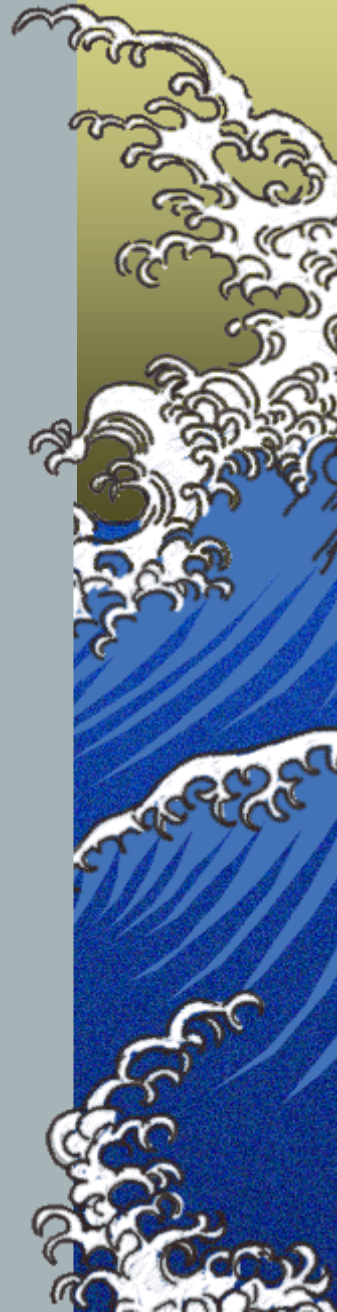
Changes to L.E. Power (con't)

▲ *BEFORE*

- *Web surfing:
Arguably Title III
warrant or 2703(d)
order*
- *Searches of Email
Content (Search
warrant or subpoena
w/ notice)*

▲ *AFTER*

- *Pen Register/Trap
and Trace Order*
- *Extended Ability to
Delay Notice*



Changes to L.E. Power (con't)

▲ *BEFORE*

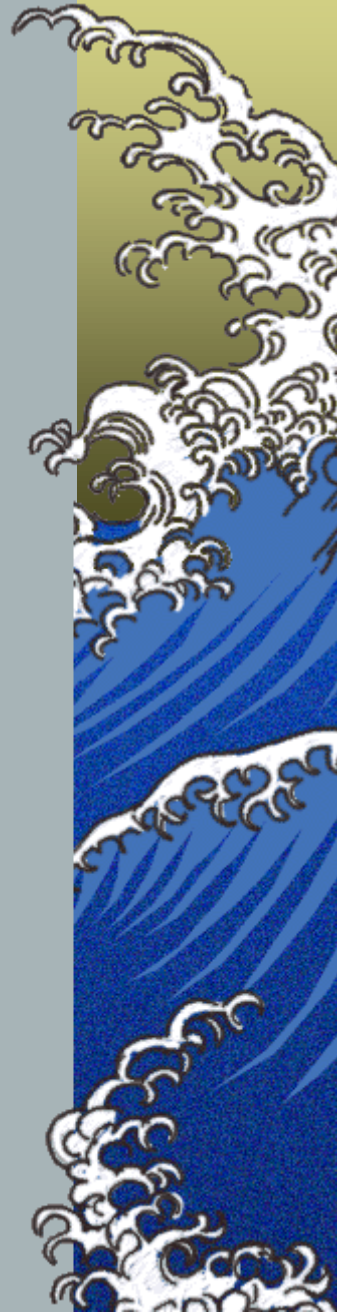
- *Wiretap authorization in district where telephone/computer is located*

- *Voicemail requires Title III Warrant*

▲ *AFTER*

- *Roving wiretaps*

- *Search warrant*



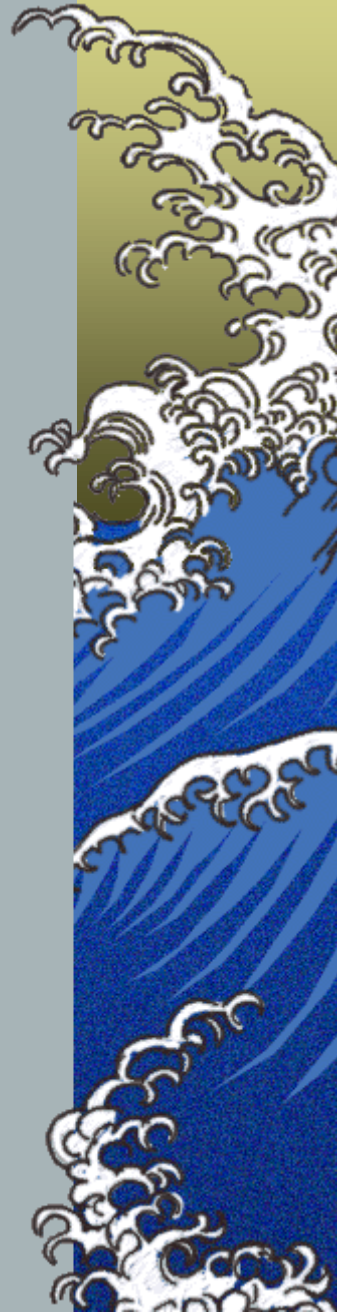
Changes to L.E. Power (con't)

▲ *BEFORE*

- *Needed court order to monitor computer users*
- *Voicemail requires Title III Warrant*

▲ *AFTER*

- *If use is “unauthorized” then L.E. may monitor with permission of system owner*
- *Search warrant*



Changes to L.E. Power (con't)

▲ *BEFORE*

- *ISPs may not disclose information to L.E. without a court order*
-

▲ *AFTER*

- *ISPs can voluntarily disclose "non-content" to L.E. w/o court order. sec. 212.*
 - *To protect provider's rights and property*
 - *Threat of death, injury*

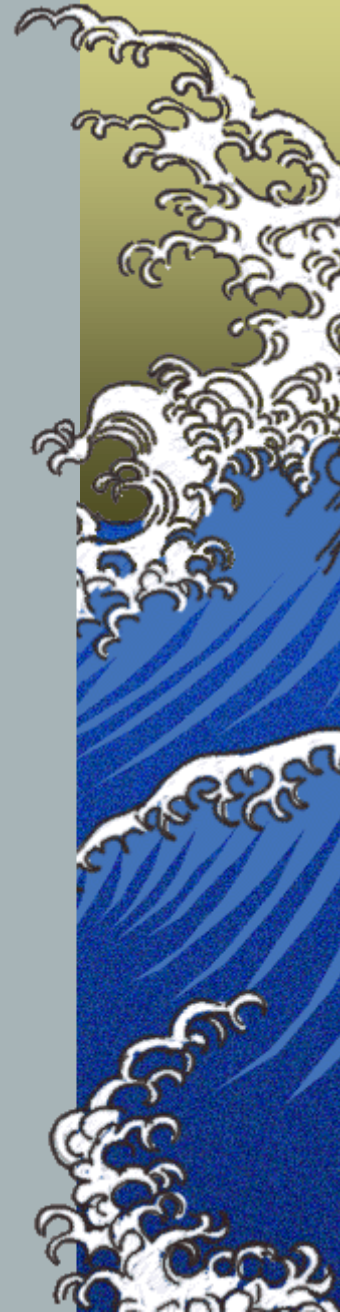


New Terrorism Offenses

▲ *Domestic Terrorism*

- `(A) involve acts dangerous to human life that are a violation of the criminal laws of the United States or of any State;
- `(B) appear to be intended--
 - `(i) to intimidate or coerce a civilian population;
 - `(ii) to influence the policy of a government by intimidation or coercion; or
 - `(iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping; and
- `(C) occur primarily within the territorial jurisdiction of the United States.'

▲ *Concern that legitimate protest activity, especially if violence occurs, will result in charges*



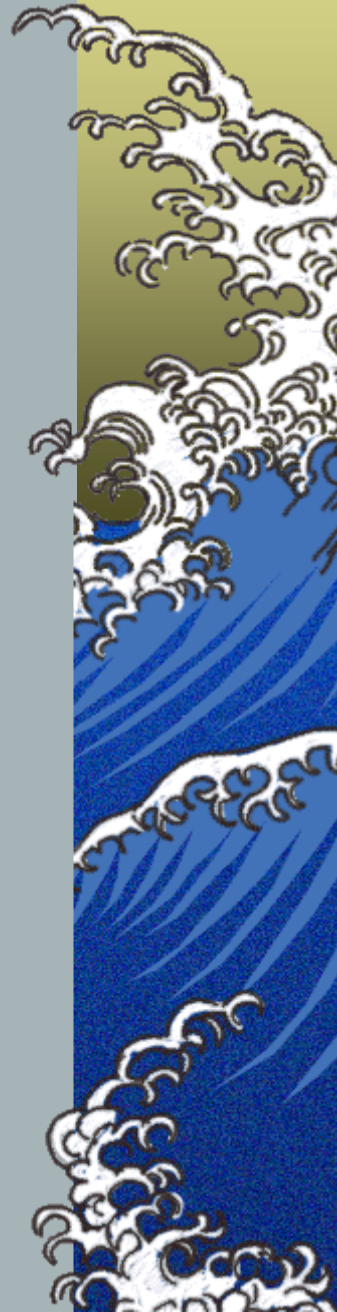
New Terrorism Offenses (con't)

▶ Some “hacking” is terrorism:

▶ 1030(a)(1) (relating to protection of computers), 1030(a)(5)(A)(i) resulting in damage as defined in 1030(a)(5)(B)(ii) through (v) (relating to protection of computers)

1030(a)(1): Obtaining classified information that could be used to harm the U.S. or disclosing info to foreign gov't

1030(a)(5)(A)(i): transmission of a program, information etc. intentionally causes damage (Medical Info, Physical injury, threat to public health or safety, gov't system for justice, defense, or security.)



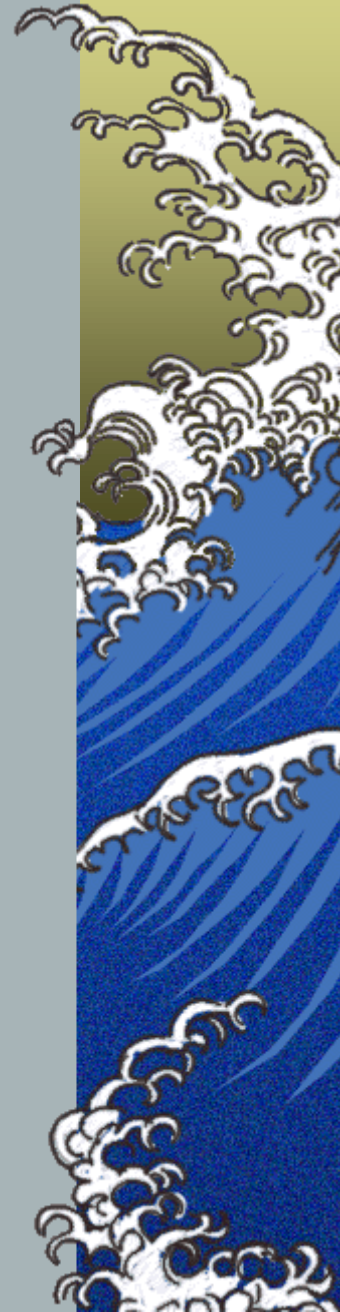
New Terrorism Offenses (con't)

- ▶ *Harboring or Concealing Terrorists*
- ▶ *Material Support for Terrorists: Includes Expert Advice or Assistance*

New Offenses = new surveillance power

Wiretapping for 1030

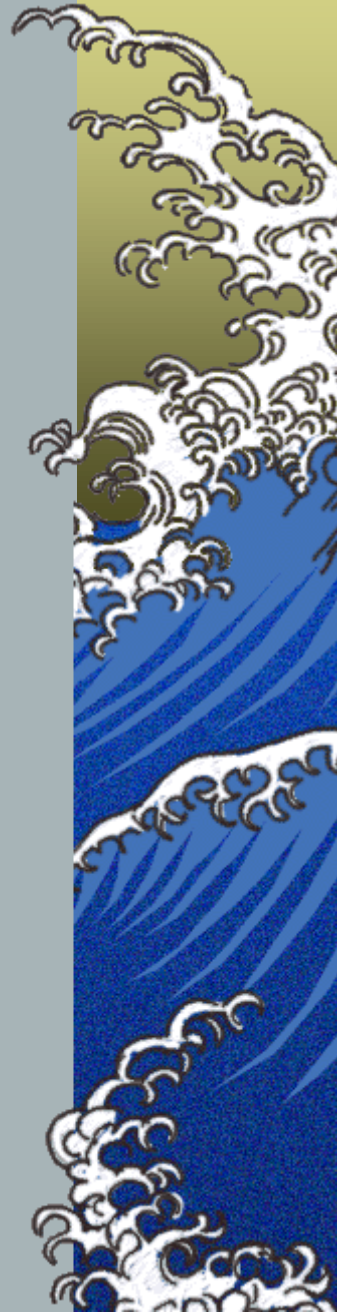
*Increased penalties:
misd now 5 yrs. 5 yrs
now 10.*



FISA

★ *Foreign Intelligence Surveillance Act:*
Allowed spying on reduced judicial oversight, showing if the purpose of surveillance was investigation of American agents of foreign gov't

Now allows if “a significant purpose” of the surveillance (218)



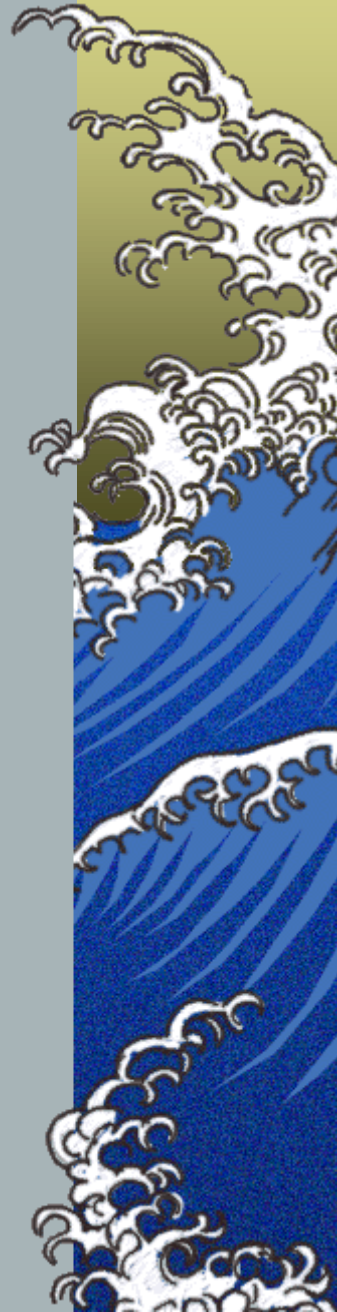
FISA

- ▶ *Allows Information Sharing Between Foreign Intelligence and L.E.*
- ▶ *LE Wiretap results*
- ▶ *Grand jury investigations (203a)*
- ▶ *FISA wiretaps w/o probable cause shared with L.E. if person suspected agent of for. gov't*



Proposed Legislation

- ▶ *Cyber-Security Enhancement Act (CSEA)*
 - ▶ *Passed House, awaiting Senate*
- ▶ *Copyright Holder “Hack Back” Legislation*
 - ▶ *Introduced in House*



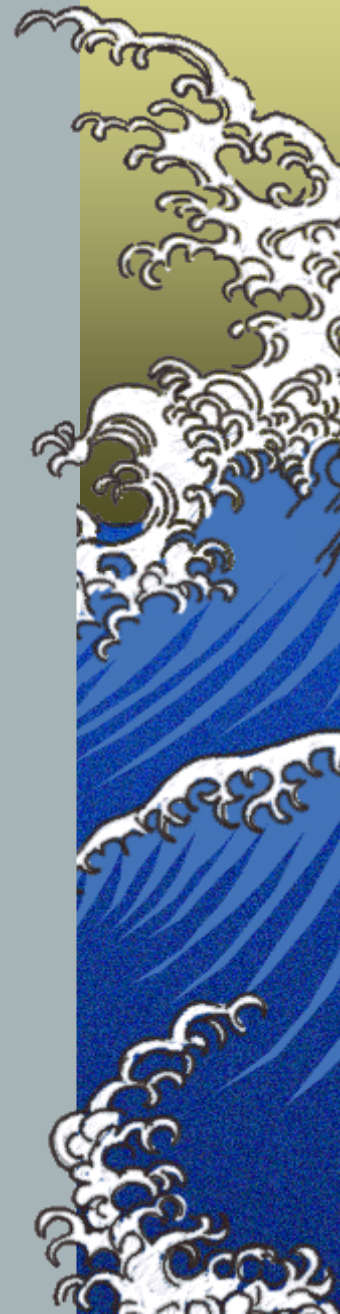
CSEA: 1030

- ▶ *Section 105* increases penalties for the (a)(5)(A)(i).
 - ▶ “[I]f the offender knowingly or recklessly causes or attempts to cause serious bodily injury from conduct in violation of subsection (a)(5)(A)(i), a fine under this title or imprisonment for not more than 20 years, or both” attaches.
 - ▶ “[I]f the offender knowingly or recklessly causes or attempts to cause death from conduct in violation of subsection (a)(5)(A)(i), a fine under this title or imprisonment for any term of years or for life, or both” attaches.



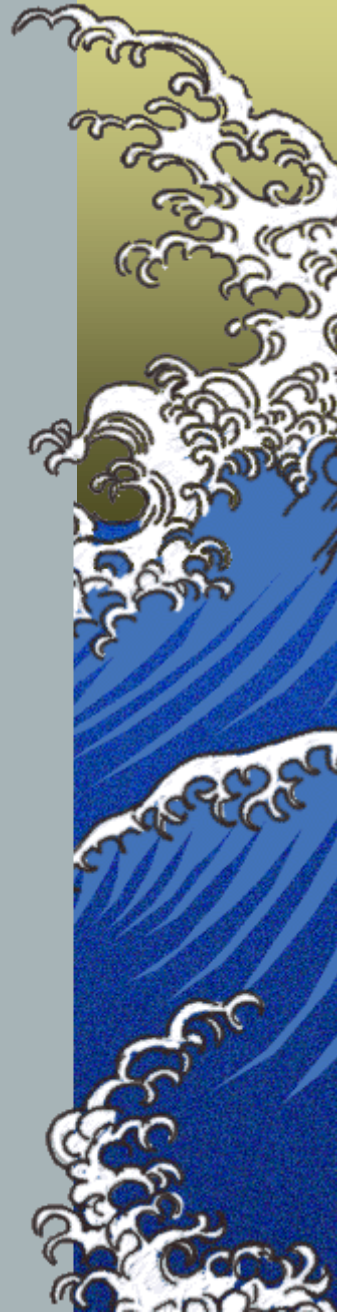
CSEA: 1030 (con't)

- ▶ *Section 101*: asks the Sentencing Commission to reevaluate § 1030 guidelines.



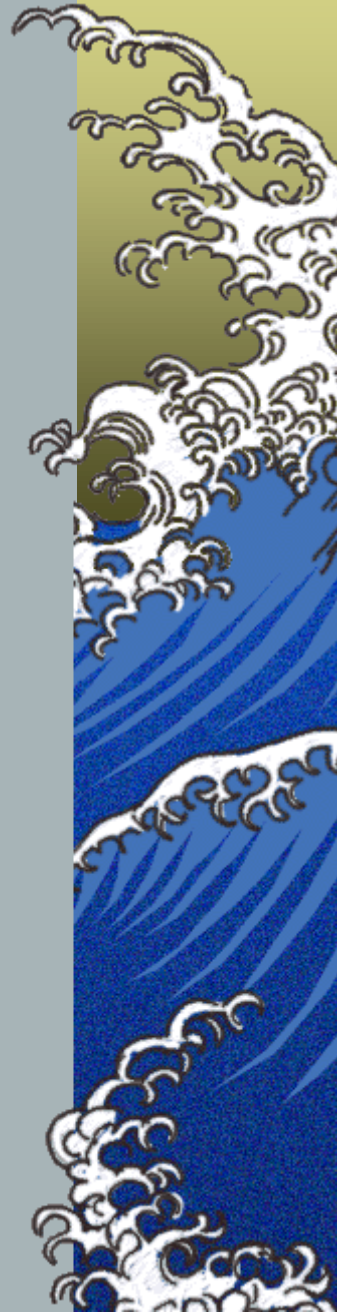
CSEA: Interception/Stored Communications

- ▶ **Section 108(a):** interception of private cell phone communications are punished same as interception of communications sent over traditional media.
- ▶ Increases penalties [from misdemeanor] to 5 years where the actor has the aggravating mental state.



CSEA: Search and Seizure

- ▶ *Section 102*: ISPs able to disclose information about a possible emergency situation in a broader range of circumstances.
 - ▶ § 2702(b)(6)(c):
 1. “Good faith” rather than “reasonable” belief of emergency.
 2. provider need not determine what is an immediate danger.
 3. Third, provider can disclose the information to any Government entity, not just law enforcement.



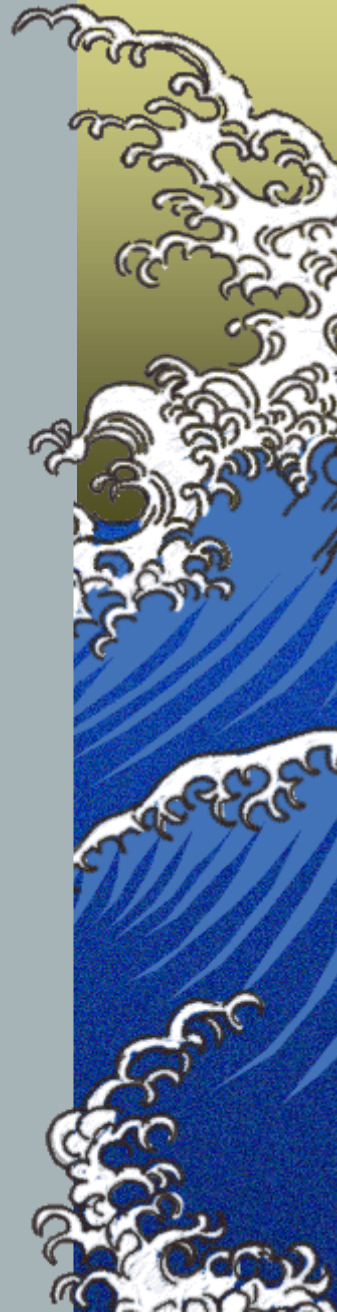
CSEA: Search and Seizure (con't)

- ★ *Section 108*: pen/trap uses in two new “emergency” situations: immediate threats to national security interests and ongoing attacks on protected computers.
- ★ *Section 103, 106*: communications providers cannot be prosecuted for computer access crimes when executing government search orders.



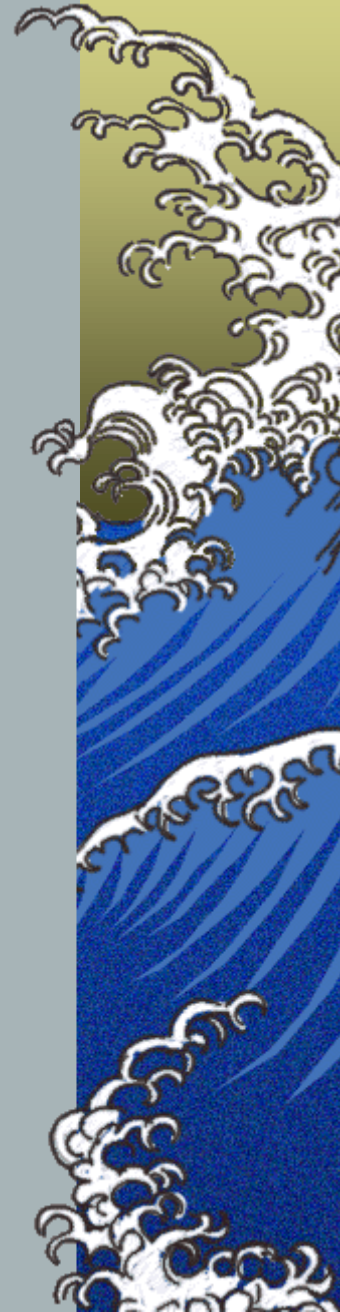
Hack Back

- ▶ limits copyright holders' civil and criminal liability for “disabling, interfering with, blocking, diverting, or otherwise impairing the unauthorized distribution, display, performance, or reproduction of his or her copyrighted work on a publicly accessible peer-to-peer file trading network.”
- ▶ Not permitted to, “without authorization, alter, delete, or otherwise impair the integrity of any computer file or data residing on the computer of a file trader.”



What Can I Do?

- **Call or Write Your Congressperson**
- **Get Educated**
 - **American Civil Liberties Union:** <http://www.aclu.org/issues/cyber/hmcl.html>
 - **Electronic Frontier Foundation:** www.eff.org/
 - **Sousveillance:** <http://wearcam.org/wsd.htm>



The End

Stanford Center for Internet & Society
cyberlaw.stanford.edu

Jennifer S. Granick
jennifer@granick.com
www.granick.com

Special Thanks to:
Matthew Scherb, Northwestern Law School

