
DEFCON
WTF Happened to the Constitution?!
The Right to Privacy in the Digital Age
Michael "theprez98" Schearer
DEFCON 19
Las Vegas, NV

Michael "theprez98" Schearer

- Founder and Owner, Leverage Consulting & Associates
- 8+ years in the U.S. Navy as an EA-6B Prowler Electronic Countermeasures Officer
  - Veteran of aerial combat missions over Afghanistan and Iraq
  - Spent 9 months on the ground in Iraq as a counter-IED specialist
- Founding member of Church of WiFi and Unallocated Space, and father of four

The Assault on Privacy

"Those who would give up Essential Liberty to purchase a little Temporary Safety, deserve neither Liberty nor Safety." Ben Franklin

Sunday, July 24, 2011

Former Minnesota Governor: TSA pat downs 'Fascist' act

From PressTV:

> Former Minnesota Governor Jesse Ventura lambasted at a federal court hearing 'un-American' security procedures implemented at airports across the nation in 2010.
>
> He filed a lawsuit with the Transportation Security Administration (TSA) in January, claiming their use of pat down searches at airport security checkpoints is unconstitutional. Pioneer Press reported that a lawyer for Ventura argued in federal court that the searches violate his Fourth Amendment right against unreasonable and unwarranted searches.
>
> The Justice Department has filed a motion to have the lawsuit dismissed, claiming that the searches are legal and that they can only be challenged in a federal appeals court.

Posted by theprez98 at 6:37 PM 0 comments +1 0

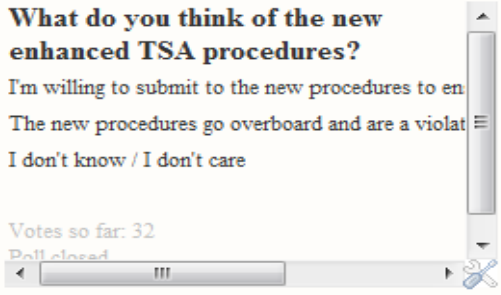
Links to this post

Man say he's mishandled by airport screener again

From the StamfordAdvocate:

> A Michigan man with bladder cancer who suffered a rough airport pat-down that caused his urostomy bag to spill its contents on his clothing last fall said he was mishandled by a screener at the same airport earlier this month.
>
> A security agent's aggressive pat-down in November caused the lid of Thomas Sawyer's bag to loosen, spilling urine on his shirt and pants. Transportation Security Administration chief John Pistole called Sawyer to apologize and pledge an investigation into how screeners handle passengers with sensitive medical conditions.

What do you think of the new enhanced TSA procedures?



ACLU Airport Security

Electronic Frontier Foundation

Electronic Privacy Information Center

FourthAmendment.com

Blog Archive

July (39)

June (32)

May (6)

April (14)

March (17)

February (54)

January (74)

December (77)

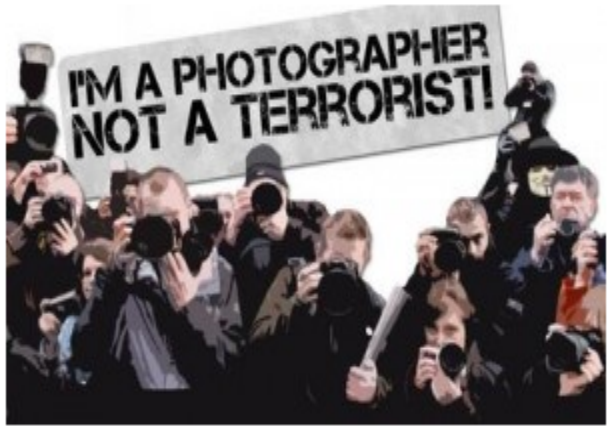
Unall{Ø}cated

← Home Design for Hackers

Ham Radio Night: Prep for Field Day! →

May Flex Your Rights Night!

Posted on May 14, 2011 by theprez98



Tuesday, May 17th will be our monthly "Flex Your Rights Night." The central purpose of Flex Your Rights Nights are to provoke discussion and focus on the legal issues surrounding individual civil rights and how to protect them as it relates to encounters with law enforcement, in the context of technology, in everyday society, or in the abstract.

For this month's Flex Your Rights Night, we will be starting at 7PM and discussing the issue of photographer's rights. Join us as we focus on the distinction between the First Amendment rights of photographers and the power of the government to restrict those

Status

The space has been closed since 02:10:12 2011-07-25

The Wall

Space & Event Location

We're located at 512 Shaw Court, Severn MD, 21144. Unless otherwise noted, events on the page happen here at the space.

Call Us!

If you need help with directions, or have questions about the space,

Why you should be skeptical

- I am not a lawyer
- My presentation is (both) unintentionally and intentionally biased by my own beliefs
- This isn't a political presentation, but it is inevitably influenced by political issues
- Bottom line: Don't take my word for it; read the source material and make up your own mind!

Part I: History

WTF HAPPENED TO THE CONSTITUTION?

"The Right to Privacy"

- What is it?
- Where does it come from?

History (1/2)

- Magna Carta (1215)
- Divine Right of Kings (~1600-88)
- Semayne's Case (1604)
- Lex, Rex (1644)
- The Glorious Revolution (1688)
- English Bill of Rights (1689)
- Paxson's Case (1760)
- William Pitt, Earl of Chatham (1763)
- Wilkes v. Wood (1763), Entick v. Carrington (1765)

History (2/2)

- Malcom Affair (1766)
- Virginia Declaration of Rights (1776)
- State Constitutions
- State Ratifying Conventions
- First Congress (1789-91)
- Bill of Rights Ratification (1791)
- Fourteenth Amendment (1868)

Magna Carta (1215)

- Proclamation by King John of certain liberties
- King's will was not arbitrary
- "NO Freeman shall be taken or imprisoned, or be disseised of his...Liberties...but by...the Law of the land."

Divine Right of Kings (1600-88)

- Monarch derives his right to rule from God
- Not subject to the people, laws, or even the Church
- Theory was used to justify absolute monarchism

Semayne's Case (1604)

- Gresham and Berisford--joint tenants
- Berisford died and left some papers to Semayne
- Sheriff of London, with a valid writ, entered the house by breaking down the doors

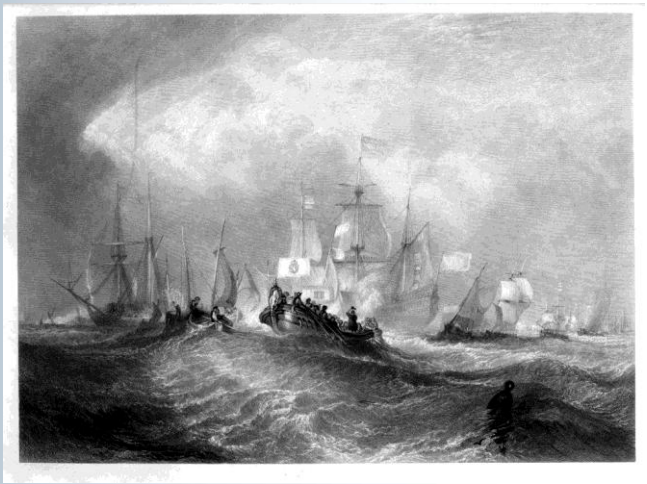
"the house of every one is to him as his castle and fortress, as well for his defence against injury and violence as for his repose."

-- Sir Edward Coke

Lex, Rex (1644)

- The Law and the Prince (or, The Law is King)
- Written by Scottish minister Samuel Rutherford
- Defends the rule of law, limited government and constitutionalism
- Attacking royal absolutism and the divine right of kings
- Charged with high treason
- Book was burned in Edinburgh, St. Andrews, and Oxford

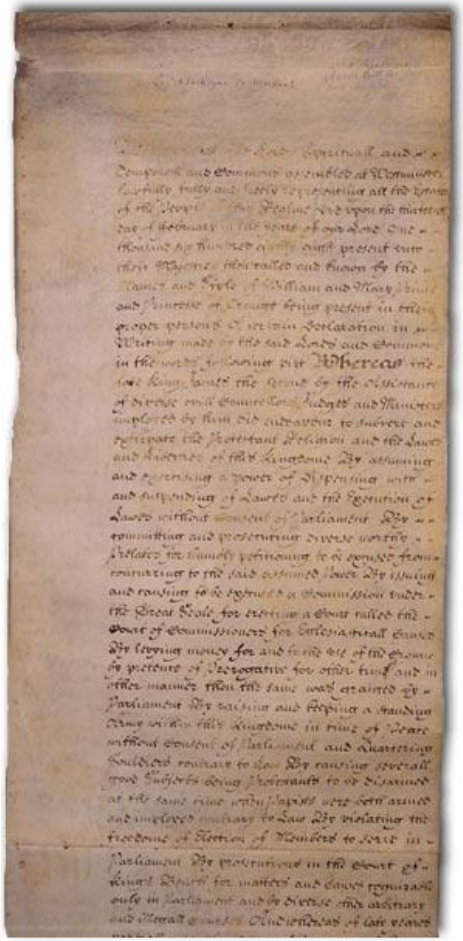
The Glorious Revolution (1688)



- Overthrow of King James II of England by English Parliamentarians and William of Orange
- The end of absolute rule by the monarchy
- Drafting of the English Bill of Rights

English Bill of Rights (1689)

- No royal interference with the law
- No taxation by Royal Prerogative
- Civil courts (not Church courts)
- Freedom of petition
- No standing army
- Right to bear arms for their own defense
- No cruel or unusual punishments, or excessive bail



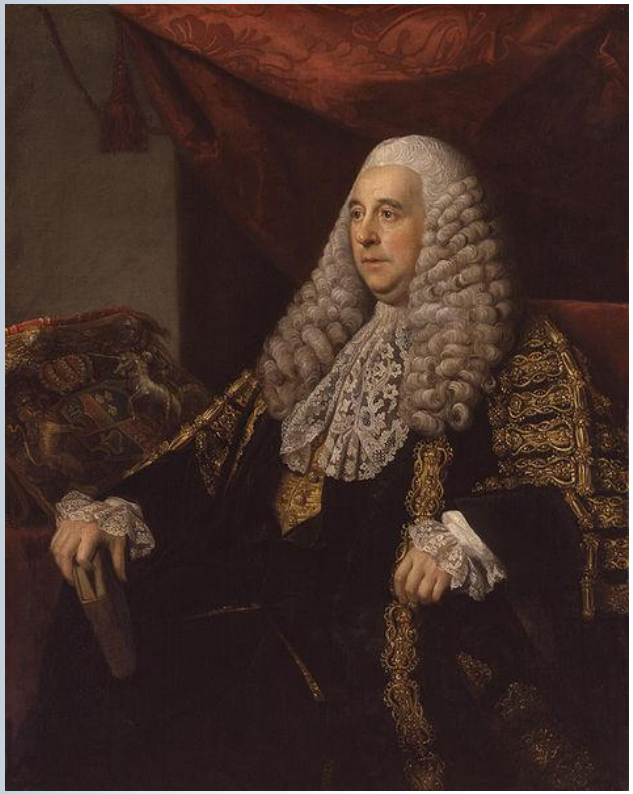
Paxson's Case (1760)

- Writs of assistance
- The death of King George II in October 1760
- Charles Paxson, British customs official
- James Otis, Jr., Boston attorney
- Outcome

William Pitt, Earl of Chatham (1763)

"The poorest man may in his cottage bid defiance to all the force of the crown. It may be frail—its roof may shake—the wind may blow through it—the storm may enter, the rain may enter—but the King of England cannot enter—all his force dares not cross the threshold of the ruined tenement."

Wilkes v. Wood (1763), Entick v. Carrington (1765)



- John Wilkes, “radical” journalist (The North Briton)
- John Entick, “radical” journalist (The Monitor)
- Lord Camden condemned the practice of general warrants

Malcom Affair (1766)

- Search of Daniel Malcom's home (and business) in Boston on a writ of assistance
- Malcom permitted the search, but not of a locked cellar
- Officials returned with a specific warrant, but Malcom locked his house
- Malcom and Otis provoking another lawsuit?

Virginia Declaration of Rights (1776)

X That general warrants, whereby any officer or messenger may be commanded to search suspected places without evidence of a fact committed, or to seize any person or persons not named, or whose offense is not particularly described and supported by evidence, are grievous and oppressive and ought not to be granted.

State Constitutions

Of the ten states that adopted constitutions between the Declaration of Independence and the Constitution:

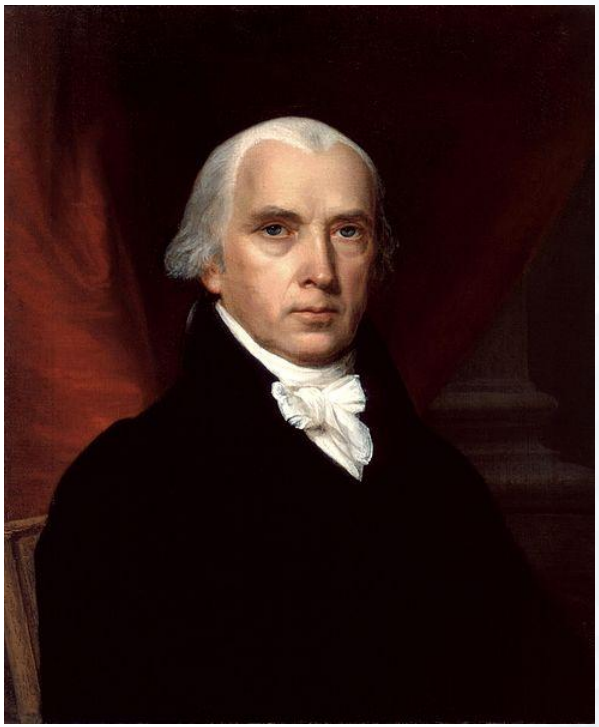
- Three expressed condemned general warrants (Virginia, Maryland, North Carolina)
- Three included provisions similar to the eventual language of the Fourth Amendment (Massachusetts, Pennsylvania, Vermont)
- Delaware, New York and New Jersey did not include any provisions resembling the eventual Fourth Amendment, but all three states did explicitly include provisions that incorporated English common law

State Ratifying Conventions

- Patrick Henry's speech, June 24, 1788, enumerated rights (Virginia)
- New York
- Rhode Island

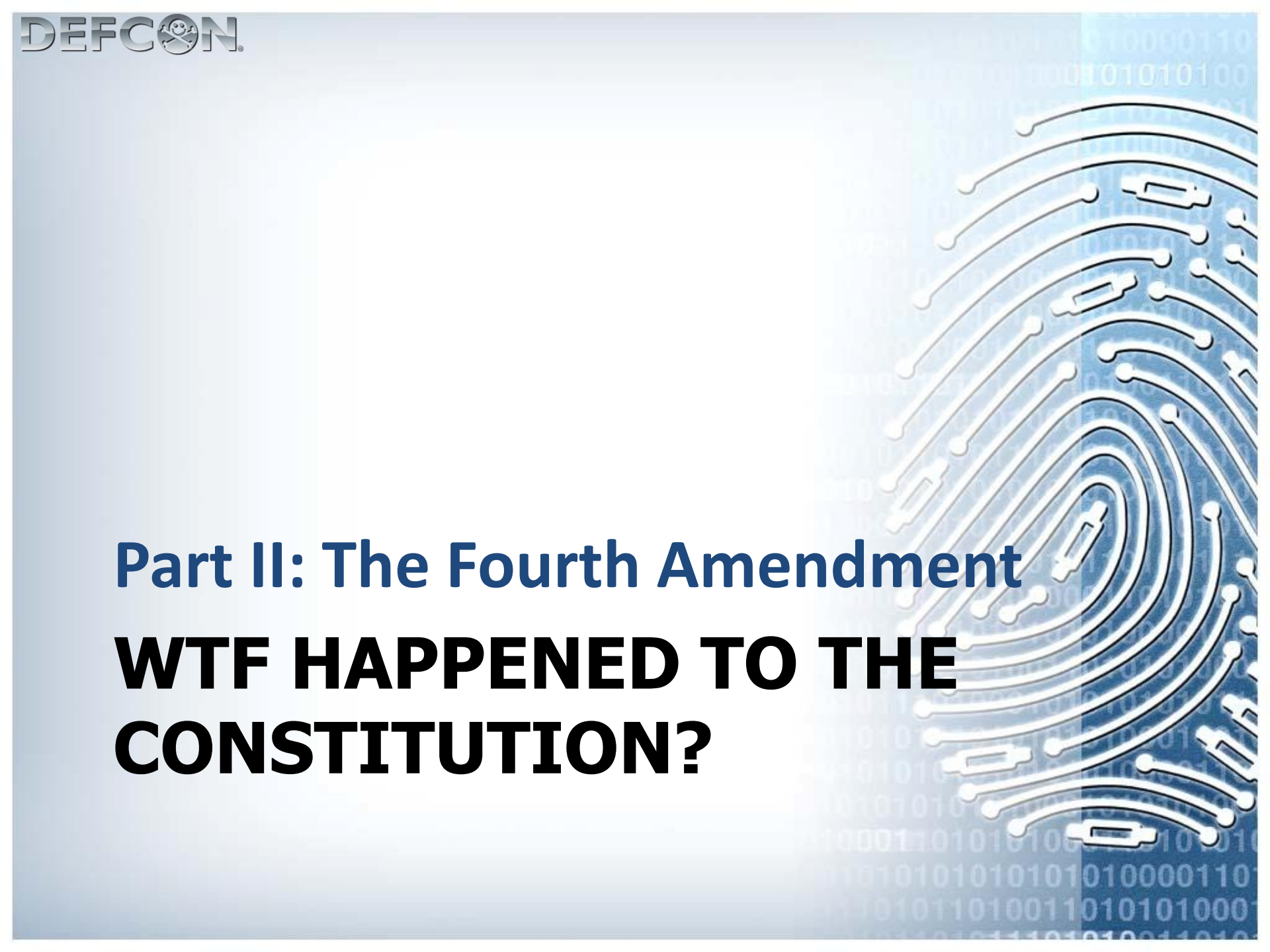
First Congress (1789-91)

- Enumerated rights vs. limited powers
- Madison's first draft
- Bill of Rights ratification (1791)



Fourteenth Amendment (1868)

- One of three Reconstruction Amendments
- Legitimize the Civil Rights Act of 1866
- Sought to overrule Dred Scott v. Sandford (1857)
- Sought to overrule Barron v. Baltimore (1833) and apply the Bill of Rights to the states
  - Privileges or Immunities Clause (Slaughterhouse Cases)
  - Due Process Clause (Wolf v. Colorado, 1949; Mapp v. Ohio, 1961)



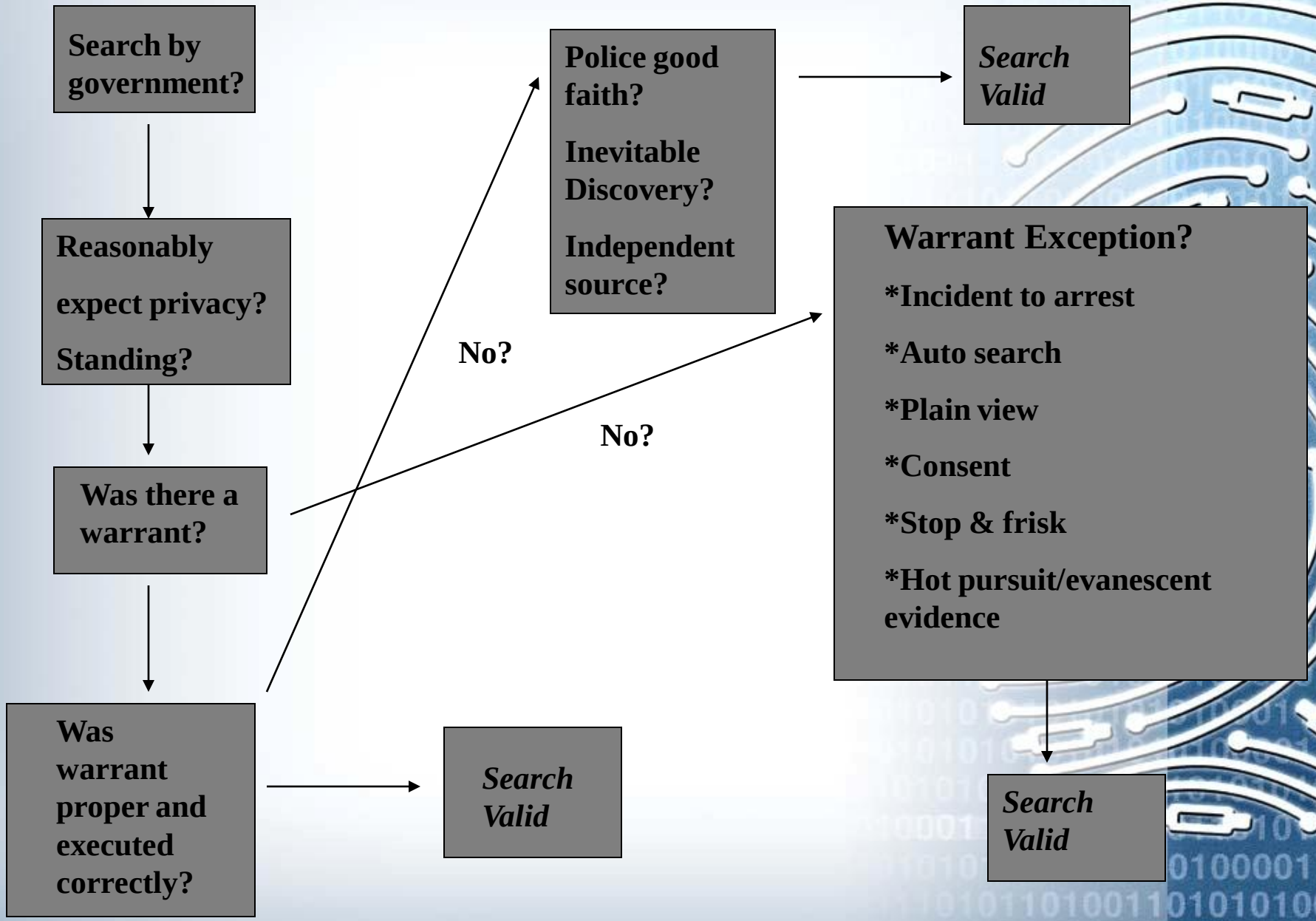
Part II: The Fourth Amendment

WTF HAPPENED TO THE CONSTITUTION?

Fourth Amendment

The right of the people to be secure in their persons, houses, papers, and effects, against **unreasonable searches** and **seizures**, shall not be violated, and no **Warrants** shall issue, but upon **probable cause**, supported by Oath or affirmation, and **particularly** describing the place to be searched, and the persons or things to be seized.


4th Amendment
Effecting Arrest
Accousting
Seizure/Stop
Arrest w/o Warrant
Prob Cause: Factors (indv to specific persons/places - Pringle): (1) Informant (a. basis of know, b. reliab of infrm, c. self-verifying?, d. inform corroborated), (2) exp of PO, (3) Ds prior crim record, (4) info from W or Vic, (5) furtive gestures or flight?, (6) nature of area, (7) common enterprise?
(1) phys restr by PO, OR (2) show of author & submission
Must have PC
Rsb Art. Suspc armed/dang or contraband
PC develops that crim ab to be comm or did
Search & Seizure Rule:
defined
Search: Person, Place, House
Government actor intrudes on rsb expct of privacy that society wld agree is private
ask
defined
Seizure
Whether state actor meaningfully interferes w/ indiv possessory interest
Public Actor or Governmental Conduct?
Private still Gov't IF under authority of PO
Reasonable Exp of Privacy & Society Wld Believe So?
Standing
yes
Own premise searched
Live in place or home (no own)
Overnight guests
Look for "meaningful connection" that's not fleeting
sometimes
Don't own but may have rsb expt of privacy (i.e. borr purse)
Passenger in cars
if
If don't claim own car
AND
Don't claim property searched
no
Held out to public everyday
Sound of voice
handwriting
Records held at bank
Emanating Odors (dog search if public & srch 4 contra)
Paint on car
Garbage (not in curtilage)
"Open Fields" & "Pub. Airspace":
Dunn Factors: (1) prox to house, (2) enclosed?, (3) nature/use of area, (4) steps to protect area
New Tech: (1) whth in gen use, (2) revealing inside not knwn othwis (arg gen use & know)
Valid Search Warrant?
1) Probable Cause
Fair prob. that evid. will be found in place searched
Hearsay permitted in probable cause
Informant tip permitted
but states
Aguiler Test:
(1) Sufficient facts & circum. to allow magis to know how PO got info
AND
(2) Police must vouch for RELIAB and CREDIB of informant (thr prev tips) – use TOT of CIRCUM
Factors: (1) Informant (a. basis of know, b. reliab of infrm, c. self-verifying?, d. inform corroborated of future behavior)?
2) Particularity items & place
In MD – daytime is rule; Fed – exp made for night
3) Reviewed/app by neutral mag
4) Signed under Oath
5) PC not stale/ old/out-dated
Serve in day, timely, knock/annc (avoid prop damag, avoid violence, prevent unnec invasion)
Executing W
all
Wait rsbl amt of time after K&A
Detain all (frisk = rsb sus of crim for non-subs)
Search only areas listed in warrant
Seize only items listed in W & in plain view
If not valid, will PO "Good Faith" reliance save?
Good faith will overcome defects with probable cause or ptc req for physical evidence
or
Magistrate is biased
Affidavit for W is so lacking in PC – no rsb PO wld rely
Affidavit for W is so lacking in part – no rsb PO wld rely
PO or pros lied or mislead magis.
If non-valid W, 6 Exceptions to Warrant Requirement:
Search Incident to Lawful Arrest:
If arrest is unlawful then search is unlawful
Arrest & search must be contemp in time & place
Geographic Scope Limitation
"Wingspan" - person & areas reached for weapon or destroy evidence
If taken out of car & arsted NO… UNLESS can reach car for weapon or dest evid
Automobile Exception:
Just b/c car, AE except not guar. – intent b/c cars move
Automobile Exception (when car has evidence):
Must have PC to support S
Can search ALL car (spaces & trunk) – less exp of privacy (Carney)
Package or container that RSB cld contain item looking for if owned by pass or driver
PC can dev after stop
Plain View
PO must be legit present when he/she does viewing of item seized & immediately apparent
Whether lawfully seeing (i.e. enter house lawfully)
Inventory srch: prtct prop, prtct claims of fraud/theft, PO safety
Must follow pre-estb PO procedures.
Consent
Consent must be:
both
Voluntary
and
Intelligent
Saying have warrant, negates consent – but no req on PO to explain
TP consent – 2 own, either can consent.
2 own, both pres & 1 does not consent then not
If consent, may limit scope (Jimeno)
Matlock Factors for TP Consent: (1) mutual use, (2) joint access/control, (3) rsbl recognition, (4) assumed risk
Police must act reasonably to determine.
Stop & Frisk
Terry Stop
BREIF deten for purp of invest suspic conduct
Standard = reasonable suspicion
Terry Frisk
Patdown check for weap/contra
Standard = reasonable suspicion for PO safety (looks like weapon or contra)
Hot Pursuit / Evanescent Evidence
Ev Evid
Evan Evid: evid that might disap if PO gets warrant (scrape fingernails)
Hot Purs
If PO are not w/in 15 min of fleeing felon then not w/in hot purs
If ok, anything entered from home will be admiss

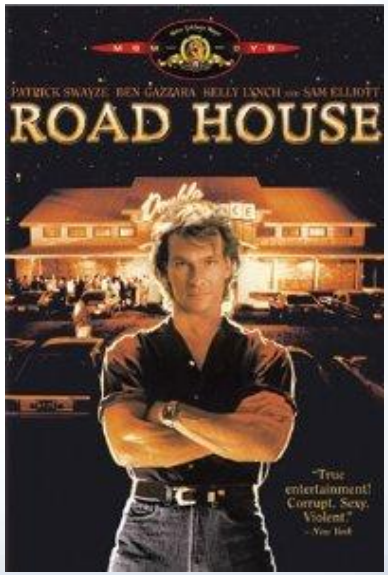

Search by government?
Reasonably expect privacy?
Standing?
Was there a warrant?
Was warrant proper and executed correctly?
Search Valid
No?
Police good faith?
Inevitable Discovery?
Independent source?
Search Valid
No?
Warrant Exception?
*Incident to arrest
*Auto search
*Plain view
*Consent
*Stop & frisk
*Hot pursuit/evanescent evidence
Search Valid

Key questions

- Was the action performed by the government?
- Was there a reasonable expectation of privacy?
- Was there a warrant?
- Was the warrant proper and executed correctly?

Was the action performed by the government?

- Someone acting in an official capacity on behalf of the federal or state government
- Can be a federal or state official, or a private individual acting on behalf of the federal or state government



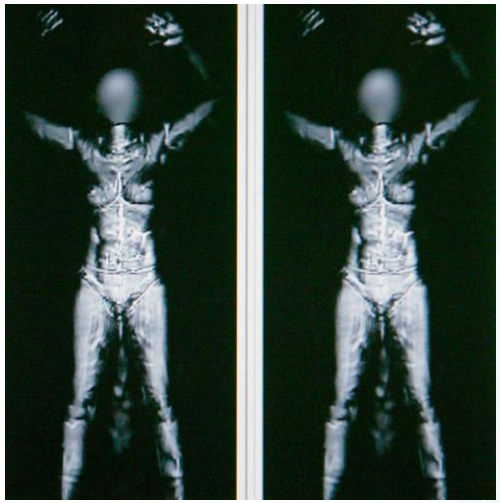
Was there a reasonable expectation of privacy?

- A government intrusion only constitutes a “search” when there is a reasonable expectation of privacy
- Otherwise, it is not a search and the Fourth Amendment does not apply

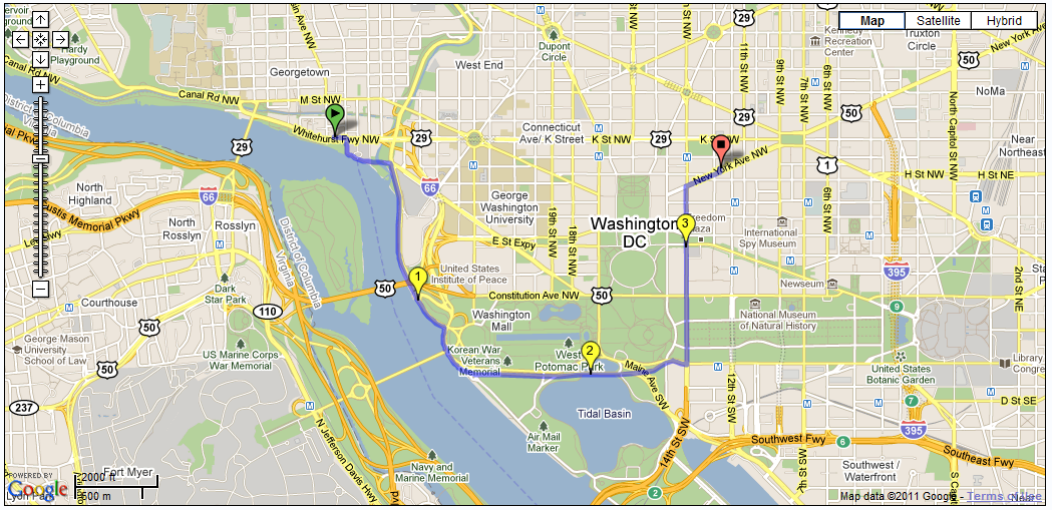
Reasonable expectation of privacy

1. Actual expectation of privacy
2. Your expectation is reasonable to society as a whole

Reasonable expectation of privacy



Reasonable expectation of privacy



Reasonable expectation of privacy

- Inside / outside (home)
- Inside / outside (container)
- Inside / outside (body)
- Content / non-content (digital)
- Private / shared (social network)

Was there a warrant?

- Consent
- Plain view
- Open fields
- Curtilage
- Exigent circumstances
- Motor vehicle

Was the warrant proper and executed correctly?

- Proper:
  - Probable cause
  - Particularity
  - Neutral magistrate
    - Signed under oath
    - PC not stale/out of date
- Execution:
  - Timely / Time of day
  - Knock and announce
  - Search only areas listed in warrant
  - Seize only items listed in warrant & plain view

Exceptions to the Exclusionary Rule

- Good faith
- Inevitable discovery
- Independent source
- Intervening acts

Burden of proof

- Reasonable suspicion
- Probable cause
- Preponderance of the evidence
- Beyond reasonable doubt

Part III: Things That Should Piss You Off

WTF HAPPENED TO THE CONSTITUTION?

Things that should piss you off

1. Administrative searches
2. Administrative warrants and subpoenas
3. Public surveillance
4. Schools and students' rights
5. Legislators, judges and technology
6. It's your fault, too

Administrative searches

- **What is it?** A search conducted as part of a general regulatory scheme
- **Why is it problematic?** Generally, administrative searches are considered reasonable if they are no more intrusive or intensive than necessary and thus not subject to further Fourth Amendment scrutiny; pre-textual for criminality
- **What can we do about it?** Demonstrate that searches are increasingly intrusive in light of current technology
- **Verdict:** tough row to hoe

DEFCON

Federal Court Rules That TSA 'Naked Scans' Are Constitutional

Jul. 15 2011 - 12:13 pm | 96,916 views | 1 recommendation | 144 comments

Last weekend, a Tennessee woman was arrested at the Nashville airport for disorderly conduct after she refused TSA security measures for her children. The woman didn't want her two children to have to go through a whole-body-imaging scanner. When a Transportation Security Administration officer told her the machines were safe, she said, "I still don't want someone to see our bodies naked."

She won't be pleased with a ruling then out of the D.C. Circuit today. This morning, the federal court ruled that the "naked scans" of air travelers do not violate Americans' constitutional rights. Privacy rights group EPIC had sued the Department of Homeland Security, alleging violations of innocent passengers' Fourth Amendment right to be free of unreasonable searches. The court says that argument doesn't fly.

In the opinion [pdf] from the D.C. Circuit Court (the Volokh Conspiracy), Judge Douglas Ginsburg writes that the advance imaging technology is not unreasonable given the security concerns on airplanes, and that people have the option to opt out for a pleasurable patdown. The court notes that some "have complained that the resulting patdown was unnecessarily aggressive," but the judges don't seem overly concerned about that. Ginsburg writes:

DEFCON

The SWAT Team Would Like to See Your Alcohol Permit

How police use regulatory inspections to conduct warrantless searches

Radley Balko | December 13, 2010

Listen to Audio Version (MP3)

In August a team of heavily armed Orange County, Florida, sheriff's deputies raided several black- and Hispanic-owned barbershops in the Orlando area. There were more raids in September and October. According to the *Orlando Sentinel*, barbers and customers were held at gunpoint, some in handcuffs, while police turned the shops upside down. A total of nine shops were raided, and 37 people were arrested.

By all appearances, these raids were drug sweeps. Shop owners told the *Sentinel* police asked where they were hiding illegal drugs and weapons. But in the end, 34 of the 37 arrests were for "barbering without a licence," a misdemeanor for which only three people have ever served jail time in Florida. Two arrests were for misdemeanor marijuana possession. Just one person was arrested on felony drug and weapon charges.

The most disturbing aspect of the raids, however, was that police didn't bother to obtain search warrants. They didn't have to. The raids were conducted in conjunction with the Florida Department of Business and Professional Regulation. Despite the guns and handcuffs, under Florida law these were licensure inspections, not criminal searches. So no warrant was necessary. Such "administrative searches" are a disturbingly common end run around the Fourth Amendment.

This sort of raid is usually conducted in bars and nightclubs under the guise of an alcohol inspection. New Haven recently sent a SWAT team to a local bar to investigate reports of underage drinking. Last week the Atlanta City Council agreed to pay a $1 million settlement to the customers and employees of a gay nightclub after a heavy-handed police raid in which 62 people were lined up on the floor at gunpoint, searched for drugs, and checked for outstanding warrants (and, incredibly, unpaid parking tickets). The September 2009 raid was conducted after undercover vice cops claimed to have witnessed patrons and employees openly having sex at the club. But the police never obtained a search warrant. Instead the raid was conducted as part of an alcohol inspection. There were no drug arrests, but eight employees were arrested for permit violations.

DEFCON

Minnesota Tenants Challenge Nosy Housing Inspectors

Jacob Sullum | December 29, 2010

Last week the Minnesota Supreme Court agreed to hear a case in which the Institute for Justice is challenging a local ordinance that lets housing inspectors roam people's apartments to make sure they're up to code. Red Wing, Minnesota, began requiring the inspections in 2006 as a condition of granting rental licenses to landlords. If a landlord or occupant does not agree to an inspection, the city can ask a judge for a warrant. But because the visits are classified as "administrative inspections," the city does not have to show there is any reason to suspect that a particular building is substandard. Armed with administrative warrants, inspectors can poke their noses into tenants' bedrooms, bathrooms, closets, and even, until a recent revision of the law, refrigerators and medicine cabinets. Although they are ostensibly looking for hazards that need to be corrected, they are expected to report evidence of certain crimes—including methamphetamine production, child abuse, elder abuse, and pet abuse—to the police. Inspectors thus can serve as proxies for the police, who would not be allowed to search people's homes without probable cause to support a criminal search warrant.

The Institute for Justice represents a group of landlords and tenants who have successfully resisted three warrant applications and argue that Red Wing's ordinance should be overturned on Fourth Amendment grounds. A judge and a state appeals court ruled that they won't have standing to mount such a challenge until the city succeeds in obtaining inspection warrants that apply to them. I.J. says the plaintiffs should not have to go through the expensive and time-consuming process of unsuccessfully resisting warrant applications before they can challenge the ordinance. It argues that they should have been allowed to seek a judgment regarding the law's constitutionality when they challenged the warrant applications and that at this point the realistic threat of unconstitutional searches is enough to give them standing. That is the issue the state Supreme Court has agreed to consider.

"Under Red Wing's rental inspection ordinance," I.J. notes, "it is easier for the government to force its way into the homes of law-abiding citizens than it is to search the home of a suspected criminal." Even people who are not worried about a stash of pot or porn might object to letting bureaucrats inspect the details of their lives. "Some people do not want government agents wandering through their homes," I.J. notes. "And for good reason. You can tell a lot about someone just from a quick walk-through of their home. According to the landlords in this case, even quick visits to rental homes reveal, among other things, a person's religious beliefs; whether they are cohabitating; whether they are messy or neat, reclusive or lonely; how much money they have; their personality; their hobbies; their social circles; and their peculiar cultural traditions and habits." The Fourth Amendment questions raised by the case have nationwide implications, I.J. says, since "these inspection programs are popping up like weeds all over Minnesota, and similar laws are appearing everywhere from California to Indiana to Pennsylvania."

Administrative warrants and subpoenas

- **What is it?** Authorizes searches for regulatory schemes, or to obtain "non-content" information
- **Why is it problematic?** Some forms of administrative warrants or subpoenas, such as National Security Letters, have very little judicial oversight; PC not required?
- **What can we do about it?** Continue to support efforts to publicize abuse
- **Verdict:** *Doe v. Ashcroft* began to rollback NSLs; but more work must continue

U.S. Department of Justice

Federal Bureau of Investigation

935 Pennsylvania Ave., N.W.
Washington, D.C. 20535

November 19, 2007

Internet Archive
116 Sheridan Avenue
San Francisco, California

To whom it may concern:

Under the authority of Executive Order 12333, dated December 4, 1981, and pursuant to Title 18, United States Code (U.S.C.), Section 2709 (Section 201 of the Electronic Communications Privacy Act of 1986) (as amended, October 26, 2001), you are hereby directed to provide to the Federal Bureau of Investigation (FBI) the subscriber's name, address, length of service, and electronic communication transactional records, to include existing transaction/activity logs and all electronic mail (e-mail) header information (not to include message content and/or subject fields), for the below-listed address holders:

[redacted]

Please see the attachment following this letter for the types of information that you might consider to be a electronic communications transactional record. We are not directing that you should provide, and you should not provide, information pursuant to this letter that would disclose the content of any electronic communication. Title 18, U.S.C., Section 2510(8) defines content as "any information concerning the substance, purport, or meaning of" a communication. Subject lines of e-mails and message content are content information and should not be provided pursuant to this letter.

If the time period noted above is to the "present," that term is intended to direct production of information to the date of the processing of this letter. If providing information to the date of processing is not feasible, please provide information to the date of receipt of this letter.

While fulfilling your obligations under this letter, please do not disable, suspend, lock, cancel or interrupt service to the above-described subscriber(s) or accounts. A service interruption or degradation may alert the subscriber(s)/account users(s) that investigative action is being taken. If you are not able to fulfill your obligations under this letter without alerting the subscriber/account user, please contact the FBI prior to proceeding.

In accordance with Title 18, U.S.C., Section 2709(b), I certify that the information sought is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, and that such an investigation of a United States person is not conducted solely on the basis of activities protected by the First Amendment to the Constitution of the United States.

In accordance with 18 U.S.C. § 2709(c)(1), I certify that a disclosure of the fact that the FBI has sought or obtained access to the information sought by this letter may endanger the national security of the United States, interfere with a criminal, counterterrorism, or counterintelligence investigation, interfere with diplomatic relations, or endanger the life or physical safety of a person. Accordingly, 18 U.S.C. § 2709(c)(1) and (2) prohibits you, or any officer, employee, or agent of yours, from disclosing this letter, other than to those to whom disclosure is necessary to comply with the letter or to an attorney to obtain legal advice or legal assistance with respect to this letter.

In accordance with 18 U.S.C. § 2709(c)(3), you are directed to notify any persons to whom you have disclosed this letter that they are also subject to the nondisclosure requirement and are therefore also prohibited from disclosing the letter to anyone else.

In accordance with 18 U.S.C. § 2709(c)(4), if the FBI asks for the information, you should identify any person to whom such disclosure has been made or to whom such disclosure will be made. In no instance will you be required to identify any attorney to whom disclosure was made or will be made in order to obtain legal advice or legal assistance with respect to this letter.

In accordance with 18 U.S.C. § 3511(a) and (b)(1), you have a right to challenge this letter if compliance would be unreasonable, oppressive, or otherwise unlawful and the right to challenge the nondisclosure requirement set forth above.

In accordance with 18 U.S.C. § 3511(c), an unlawful failure to comply with this letter, including any nondisclosure requirement, may result in the United States bringing an enforcement action.

You are requested to provide records responsive to this request personally to a representative of the FBI [redacted] or through use of a delivery service or through secure fax within fourteen (14) business days of receipt of this letter.

Any questions you have regarding this request should be directed only to the FBI [redacted] depending on whether the service is personal or through a delivery service. Due to security considerations, you should neither send the records through routine mail nor disclose the substance of this request in any telephone conversation.

Your cooperation in this matter is greatly appreciated.

Sincerely,

Arthur M. Cummings II
Deputy Assistant Director
Counterterrorism Division

IN THE UNITED STATES DISTRICT COURT FOR THE

EASTERN DISTRICT OF VIRGINIA

Alexandria Division

IN THE MATTER OF THE §2703(d) ORDER RELATING TO TWITTER ACCOUNTS: WIKILEAKS, ROP_G; IOERROR; AND BIRGITTAJ	)))))	MISC. NO. 10GJ3793

ORDER TO UNSEAL THE
ORDER PURSUANT TO 18 U.S.C. §2703(D)

This matter having come before the Court pursuant to an application under Title 18, United States Code, §2703(d), it appearing that it is in the best interest of the investigation to unseal the Court's Order of December 14, 2010 and authorize Twitter to disclose that Order to its subscribers and customers, it is hereby ORDERED that the above-captioned Order of December 14, 2010 pursuant to 18 U.S.C. §2703(d) be UNSEALED and that Twitter is authorized to disclose such Order. In all other respects, the Court's Order of December 14, 2010 remains in effect.

THE HONORABLE THERESA C. BUCHANAN
UNITED STATES MAGISTRATE JUDGE

Date: 1/5/11

Alexandria, Virginia

DEFCON

DOJ's "hotwatch" real-time surveillance of credit card transactions

A 10 page Powerpoint presentation (pdf) that I recently obtained through a Freedom of Information Act Request to the Department of Justice, reveals that law enforcement agencies routinely seek and obtain real-time surveillance of credit card transaction. The government's guidelines reveal that this surveillance often occurs with a simple subpoena, thus sidestepping any Fourth Amendment protections.

Background

On October 11, 2005, the US Attorney from the Eastern District of New York submitted a court filing in the case of In re Application For Pen Register and Trap and Trace Device With Cell Site Location Authority (Magistrate's Docket No. 05-1093), which related to the use of pen register requests for mobile phone location records.

In that case, the US Attorney's office relied on authority they believed was contained in the All Writs Act to justify their request for customer location information. In support of its claim, the office stated that:

> Currently, the government routinely applies for and upon a showing of relevance to an ongoing investigation receives "hotwatch" orders issued pursuant to the All Writs Act. Such orders direct a credit card issuer to disclose to law enforcement each subsequent credit card transaction effected by a subject of investigation immediately after the issuer records that transaction.

A search of Google, Lexisnexis and Westlaw revealed nothing related to "hotwatch" orders, and so I filed a FOIA request to find out more. If the government "routinely" applies for and obtains hotwatch orders, why wasn't there more information about these.

Public surveillance

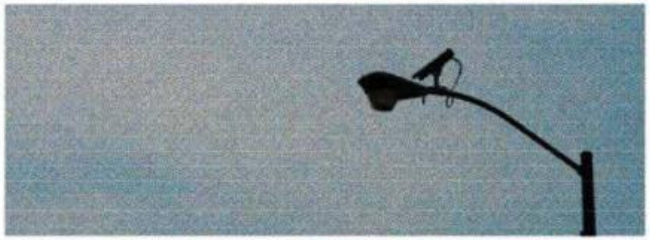
- **What is it?** Surveillance cameras, GPS tracking, marking our every move
- **Why is it problematic?** Long term surveillance, technology increases the intrusion even in public spaces; amassing of data without suspicion
- **What can we do about it?** Use privacy-enhancing technologies to our advantage; publicize known and obvious abuses
- **Verdict:** Are we too far down the slippery slope?

CHICAGO'S VIDEO SURVEILLANCE CAMERAS: A PERVASIVE AND UNREGULATED THREAT TO OUR PRIVACY

a report from the

ACLU of Illinois

February 2011

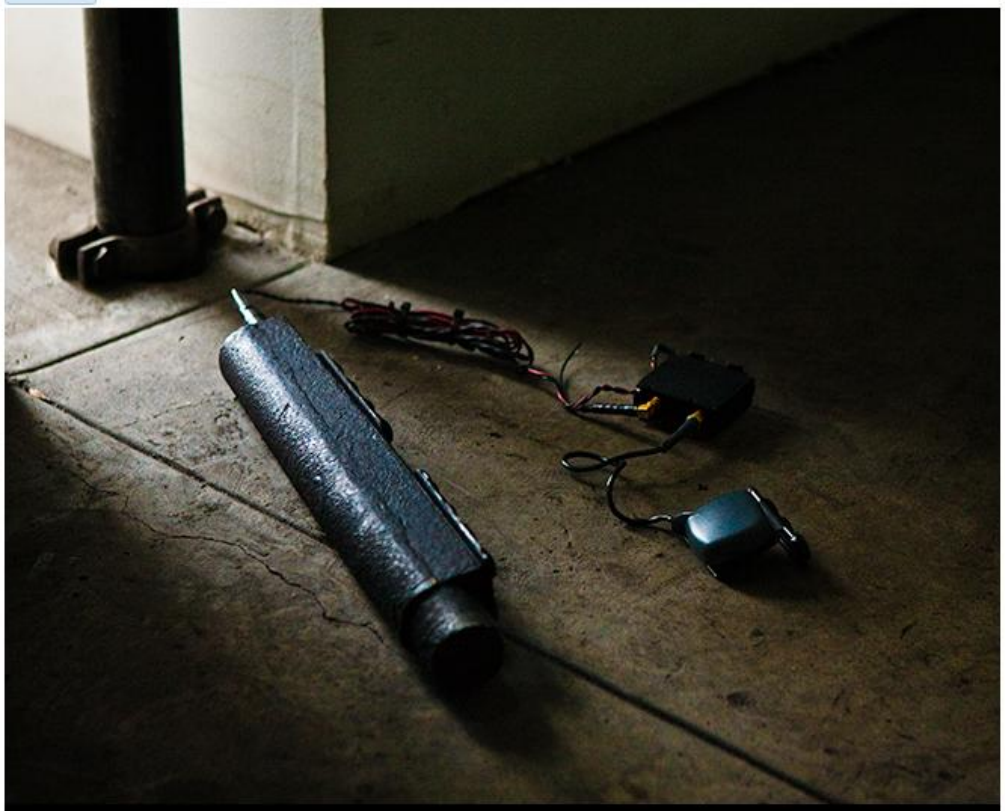


DEFCON

Supreme Court to Decide Constitutionality of Warrantless GPS Monitoring

By David Kravets June 27, 2011 | 10:27 am | Categories: Surveillance, The Courts

Follow @dmkravets · 1,661 followers



An abandoned FBI vehicle-tracking device. Photo: Jon Snyder/Wired.com

At the Obama administration's urging, the Supreme Court agreed Monday to review whether the government, without a court warrant, may affix GPS devices on suspects' vehicles to track their every move.

The Justice Department told the justices that "a person has no reasonable expectation of privacy in his movements from one place to another," (.pdf) and demanded the justices undo a lower court decision that reversed the conviction and life sentence of a cocaine dealer whose vehicle was tracked via GPS for a month without a court warrant.

DEFCON

Using hidden cameras to catch car thieves

License Plate Reader technology in place at nearly 40 law enforcement agencies across region

June 22, 2011 | By Don Markus, The Baltimore Sun

Sgt. Julio Valcarcel wheels his unmarked sport utility vehicle south onto U.S. 1 in Jessup as motorists whiz by in the opposite direction. The Maryland state trooper is not looking to ticket speeders, but rather is on the hunt for stolen cars.

And he doesn't have to consult a "hot sheet" to compare license plate numbers, or even remember the make, model and color of vehicles on the stolen-car list.

Images of license plates pop onto his laptop computer screen as the cars go by. An alarms sounds when the computer finds a stolen plate or car, or even a revoked or suspended registration, information stored in a database updated daily by the FBI and the Maryland Motor Vehicle Administration.

"It's constantly taking pictures, looking for license plates," said Valcarcel, who has spent 21 years as a trooper and is now the technical manager of the license plate reader program. "There might not be a violation at the time we capture that read, but the read might be helpful for investigative purposes down the road."

State police have been using the plate reader technology since 2004, but the program is getting a new influx of money — including a $2 million state grant last summer — doubling the funding. Officials give the devices part of the credit for a nearly 40 percent drop in car theft across the state in the past three years.

But the system has limits.

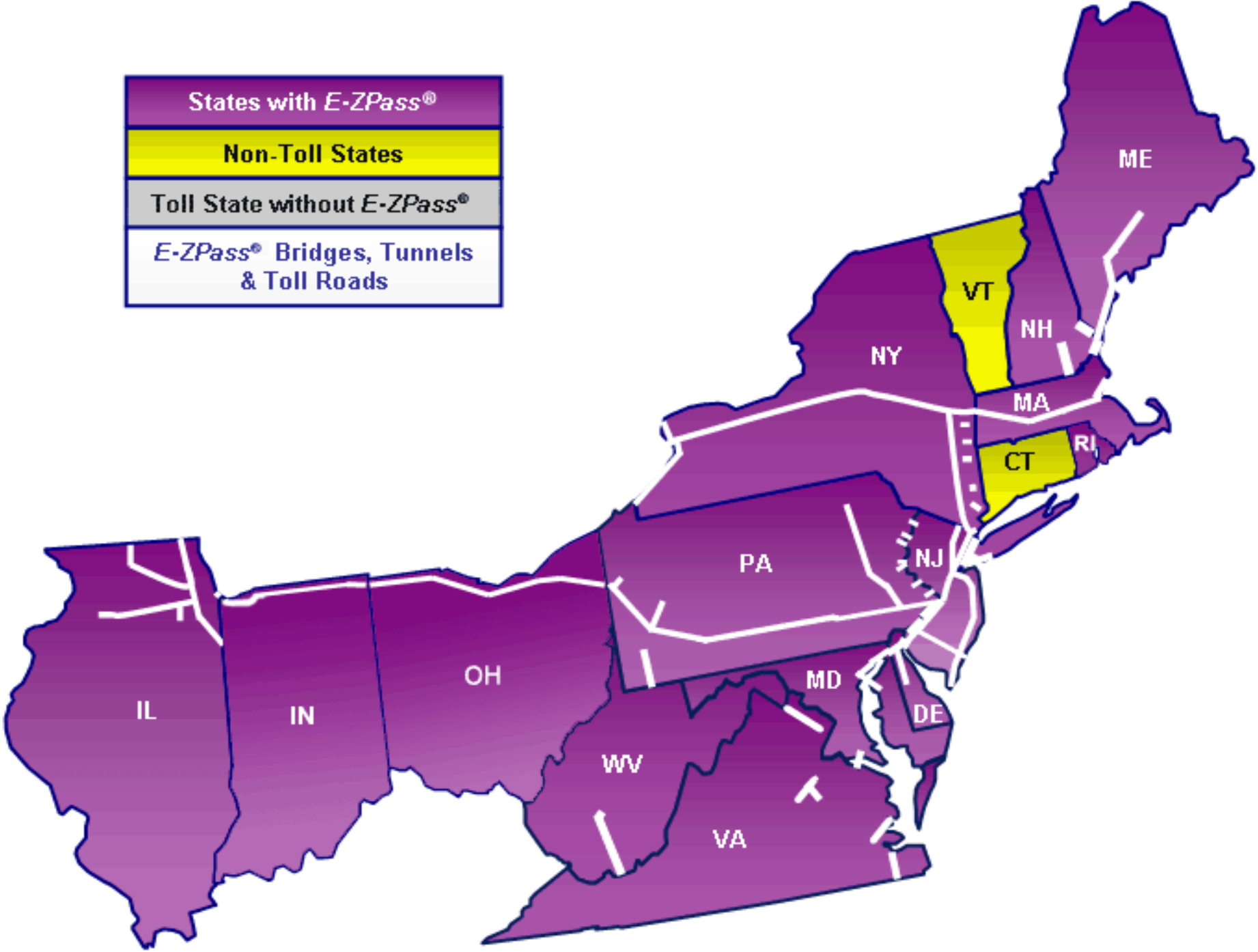
Hours after Maryland State Police Trooper Shaft S. Hunter was killed on Interstate 95 on May 21 when his cruiser slammed into the back of a tractor-trailer while chasing a speeding motorcycle, authorities said they hoped to identify the motorcycle's driver using a license plate reader. There is a stationary reader on the highway near Route 32, close to the crash site.

Valcarcel said that reading smaller motorcycle tags is more difficult than license plates on cars or trucks. The reader can't scan numbers on vehicles exceeding 120 mph or motorcycle tags that have been mounted inside wheel wells or are obscured by fenders.

Doug Ward, who spent 27 years with the Maryland State Police and now is the director of the Johns Hopkins School of Public Safety, said that racing motorcycles, sometimes speeding at 160 mph, are as big a blur to the plate readers as they are to the motorists they pass.

Ward said that plate readers used at toll plazas often have a difficult time reading tag numbers on motorcycles that are stationary, let alone motorcycles traveling at triple-digit speeds.

Valcarcel said police agencies typically keep the information for up to a year before removing it from the system.


States with E-ZPass®
Non-Toll States
Toll State without E-ZPass®
E-ZPass® Bridges, Tunnels & Toll Roads
ME
VT
NH
NY
MA
RI
CT
PA
NJ
MD
DE
OH
IL
IN
WV
VA

Schools and students' rights

- **What is it?** Students are often denied the same basic rights as other citizens
- **Why is it problematic?** While there are legitimate concerns about disrupting an educational environment, this reason is often used as a pretext to invade students' civil rights
- **What can we do about it?** Parents must continue to stay informed about their children and stand up for their rights
- **Verdict:** Students rights have eroded since *Tinker*

'Bong Hits 4 Jesus': Student Protest Goes to Supreme Court

By SUSAN DONALDSON JAMES
March 15, 2007

Joseph Frederick, a student rebel halfway through his senior year of high school, tried the patience of his principal when he displayed a drug-referenced sign reading "Bong Hits 4 Jesus" at a public parade in Juneau, Alaska, in 2002.

The 18-year-old had fashioned a 14-foot paper banner, which he held as the Olympic torch passed across the street from his high school on a national relay leading up to the 2002 winter games in Salt Lake City.

Frederick said he wanted to capture the attention of TV cameras -- and the ire of his principal.

Principal Deborah Morse, who had previously disciplined Frederick for other acts of protest, confiscated the banner and suspended Frederick, sparking a feud that has gone all the way to the Supreme Court.

Monday, the Court will hear arguments on Morse v. Frederick, in what legal experts say could be the most significant case on student free speech since the days of Vietnam War protests.

At stake is the 1969 landmark ruling Tinker v. Des Moines, which said that students do not "shed their constitutional rights to freedom of speech or expression at the schoolhouse gate."

Since then, the Court has narrowed that ruling, giving schools the right to censor speech to maintain order and protect students from harmful messages.

DEFCON

Are Student Cell Phone Records Discoverable?

Joshua A. Engel | All Articles
Law Technology News | July 19, 2011

Image by robzand

The debate over when officials can search a student's cell phone is an emerging e-discovery issue. This is illustrated in the recent case *N.N. v. Tunkhannock Area School District*, Civil Action No. 3:10-CV-1080, U.S. District Court for the Middle District of Pennsylvania.

In this case, a student at Tunkhannock Area High School in Tunkhannock, Pa., violated a school policy requiring cell phones to be turned off and stored in lockers during the school day by placing a call from her cell phone while on school property. A teacher confiscated the phone. School officials then examined the contents of the cell phone and discovered what appeared to be inappropriate photographs stored in the phone's memory.

The phone was turned over to the police. The court opinion states that, "Aside from one photograph taken by a female friend, the photographs were taken by [the student] alone, and were intended for the sole consumption of herself and her long-term boyfriend. The photographs were taken off school property, were saved to the cell phone, were never e-mailed or uploaded to the internet, and were not shared with other students."

While the police did not seem intent on pursuing charges -- a detective allegedly told the student that "had she only waited until her 18th birthday, she could have submitted the photographs directly to *Playboy* magazine instead of getting in trouble -- the district attorney took the matter more seriously. He wrote a letter to the student threatening to bring child felony pornography charges against her unless the student (and some others) completed a re-education course on sexual violence and victimization.

The student filed a lawsuit claiming that the actions of the school, the district attorney, and the police violated her First and Fourth Amendment rights.

The court has a long discussion of prosecutorial and qualified immunity issues. But what is significant from my perspective is that the court will allow the claims that the school, police, and the district attorney illegally seized and searched the student's phone.

Texas 'Calorie Camera' Will Track How Much Students Eat

By PAUL J. WEBER | 05/11/11 10:40 PM ET | AP

SAN ANTONIO -- Smile, schoolchildren. You're on calorie camera.

Health officials trying to reduce obesity and improve eating habits at five San Antonio elementary schools unveiled a $2 million research project Wednesday that will photograph students' lunch trays before they sit down to eat and later take a snapshot of the leftovers.

A computer program then analyzes the photos to identify every piece of food on the plate – right down to how many ounces are left in that lump of mashed potatoes – and calculates the number of calories each student scarfed down.

The project, funded by a U.S. Department of Agriculture grant, is the first of its kind in the nation. The cameras, about the size of pocket flashlights, point only toward the trays and don't photograph the students. Researchers say about 90 percent of parents gave permission to record every morsel of food their child eats.

"We're trying to be as passive as possible. The kids know they're being monitored," said Dr. Roger Echon, who works for the San Antonio-based Social & Health Research Center, and who is building the food-recognition program.

Here's how it works: Each lunch tray gets a bar code sticker to identify a student. After the children load up their plates down the line – cole slaw or green beans? french fries or fruit? – a camera above the cashier takes a picture of each tray.

DEFCON

School-Webcam Spy Scandal Resurfaces

By David Kravets June 8, 2011 | 12:48 pm | Categories: Surveillance, privacy

Follow @dmkravets · 1,662 followers

A suburban Philadelphia school district embroiled in a webcam spy scandal was hit Tuesday with new allegations that a student-issued laptop secretly recorded more than 8,000 images.

The latest accusations, which were said to occur during a six-month period ending September 2008, has left the high school student "shocked, humiliated and severely emotionally distressed," (.pdf) according to a federal invasion-of-privacy lawsuit, which seeks unspecified monetary damages.

As part of an FBI investigation and a lawsuit brought by a different student, a judge had contacted the boy's parents informing him of the breach, and invited them to view the pictures. The youth's parents were shown 4,404 webcam photographs and 3,978 screenshots captured with the Lower Merion School District–issued MacBook.

The amount of photos represents the largest publicly known number of images secretly recorded in the webcam scandal.

The latest lawsuit follows the October out-of-court settlement in which the district agreed to pay $610,000 to end two privacy lawsuits brought by two students who were also victims of the webcam spying scandal.

Legislators, judges and technology

- **What is it?** Many legislators and judges show little aptitude for understanding technology that
- **Why is it problematic?** Technologically incompetent legislators write poor laws, judges make poor decisions; ultimately, the justice system becomes undermined
- **What can we do about it?** Technology education, technology courts, run for office yourself?
- **Verdict:** an uphill battle, but one worth fighting

DEFCON

Cell phone measure targets ID theft threat

By Mike Wereschagin, TRIBUNE-REVIEW
Tuesday, May 29, 2007

About the writer

Mike Wereschagin is a Pittsburgh Tribune-Review staff writer and can be reached at 412-320-7900 or via e-mail.

Ways to get us

Be a Facebook fan
Follow us on Twitter
E-mail Newsletters
On your mobile

Using a cell phone to take snapshots or video of personal information should be a crime, according to a Lawrence County lawmaker who fears this rare form of identity theft might one day crop up in Pennsylvania.
Rep. Chris Sainato, D-New Castle, doesn't know anyone who's been victimized by such covert photography, but he said it's better to be safe than sorry.

The threat, Sainato said, is of a person taking a cell phone photo of a person's credit card, or using the video recorder available on some phones to steal a personal identification number from someone using an ATM.

"Cell phones are so tiny, they can do it with you standing right next to them and you might not even know they're taking a picture. That's kind of hard to do with an old-fashioned camera," said Sainato, who represents parts of Beaver and Lawrence counties.

The law would make it a third-degree misdemeanor for someone to snap an illegal photo or transmit that private information from the phone to another device, such as a computer or another phone. The House Judiciary Committee approved the bill last Tuesday, and Sainato said he expects the full House to vote on it in June.

The state Attorney General's Office hasn't prosecuted this type of identity theft, though the number of identity theft cases overall is rising rapidly, spokesman Nils Frederickson said.

"We prosecuted 301 identity theft cases last year. That's twice as many as two years before," Frederickson said. "The cases we deal with mostly involve things from Dumpster-diving to misdirection of mail."

Dumpster-diving involves someone going through another person's trash, looking for bank statements, credit card bills or anything else with confidential information on it. Misdirection of mail involves a thief filing a change of address form for someone else, then taking personal information or ordering new credit cards in the victim's name.

Cell phone-aided identity theft probably makes up "less than one-tenth of 1 percent" of all identity theft crimes, said Jay Foley, executive director of the San Diego-based nonprofit Identity Theft Resource Center. The center researches identity theft methods and trends.

"It's so rare an occurrence, I wonder why anyone would go through the trouble of creating a law for it," Foley said.

U.S. Faces Legal Challenge to Internet-Domain Seizures

By David Kravets | June 13, 2011 | 5:22 pm | Categories: Censorship, The Courts

One of Spain's most popular websites, whose American domains were seized as part of a crackdown on internet piracy, asked a U.S. judge Monday to return its property that it claims was wrongly taken.

The Rojadirecta .com and .org domains were seized in January along with eight others connected to broadcasting pirated streams of professional sports.

The legal filing in New York federal court by site owner Puerto 80 Projects represents what is believed to be the first courthouse challenge to "Operation in Our Sites." Commenced last year, U.S. Immigration and Customs Enforcement has seized as many as 208 domains the authorities claim are linked to intellectual-property fraud.

Puerto 80, which claims the Rojadirecta site sports 865,000 registered users, said it has committed no copyright infringement. The site is a discussion board where members can talks sports, politics and other topics, and it additionally links to sports streams — some of which is pirated.

Judge Who Doesn't Understand Technology Says WiFi Is Not A Radio Communication

from the *seriously?* dept

Wireless
by Mike Masnick
Fri, Jul 1st 2011
12:44pm

2
Flattr

Filed Under: data, ecpa, open wifi, radio communication, street view, wifi, wireless, wiretapping
Companies: google

Permalink.

Well, this is disappointing. As you probably know, about a year ago, Google admitted to accidentally collecting some data from open WiFi networks via its Google Street View cars. The cars were setup not just to photograph streets, but to do some location-based tracking by cataloging WiFi networks (a very common location setting technique). If you understand basic technology, you can understand what they were doing, and how it was almost certainly not to capture data from the network, but just to determine location info. Furthermore, the only data it collected was from *open* WiFi networks where people were transmitting unencrypted data *in the open*. This was data that was being *broadcast*.

But, lots of people don't understand technology and people around the world, including in governments, freaked out about this data collection. So, of course, people started filing highly questionable class action lawsuits. As more and more such lawsuits were filed, they were all consolidated into a single court. Earlier this year, we noted that the judge was trying to determine if Google's actions amounted to an illegal wiretap under ECPA (the Electronic Communications Privacy Act).

If you understand how wireless networks work, the idea that this is wiretapping is hilarious. And wrong. This is data that is broadcast in the open. *Anyone* can read it. You don't need special equipment or anything. You just need basic software to see what data is traveling across the network.

Tragically, the judge has gone the other way on this point (so far). Google had asked for the wiretapping/ECPA claim to be dismissed, as it claimed (quite reasonably) that it wasn't wiretapping. The judge put together an astoundingly confused ruling that decides otherwise. While the link here blames the wording of ECPA, which is certainly partly to blame, I think the judge's confusion over the technology is equally at fault. Basically, it's true that ECPA is somewhat vaguely worded, but it does say that:

Specialty courts

- Bankruptcy Courts
- U.S. Court of International Trade
- U.S. Court of Federal Claims
- Court of Appeals for Veterans' Claims
- U.S. Court of Appeals for the Armed Forces

- Technology Courts?

It's your fault, too

- **What is it?** We share a lot of information voluntarily
- **Why is it problematic?** By openly sharing so much information, we lower the overall societal expectation of privacy and thus subject ourselves to more governmental intrusion
- **What can we do about it?** Just because we can share, doesn't mean we have to
- **Verdict:** Another case where we might be too far down the slope to reverse course

Voluntary disclosure of privacy

amazon.com

bing

rio hotel, las vegas, nv

Maps

Web Places News Blogs Images Videos Maps

Directions My places Map apps Road Bird's eye Traffic Print Share

Twitter Maps

Timeline Search

50 most recent Tweets in this area

336 total Tweets here in past 14 days

jHarmonyP

My goal is to figure out the rubik cube #serioustweet

about 8 hours ago from Mobile Web

JuiicyGee

Piggin out with the cuzns at the #Rio buffet :)

about 16 hours ago from Twitter for iPhone

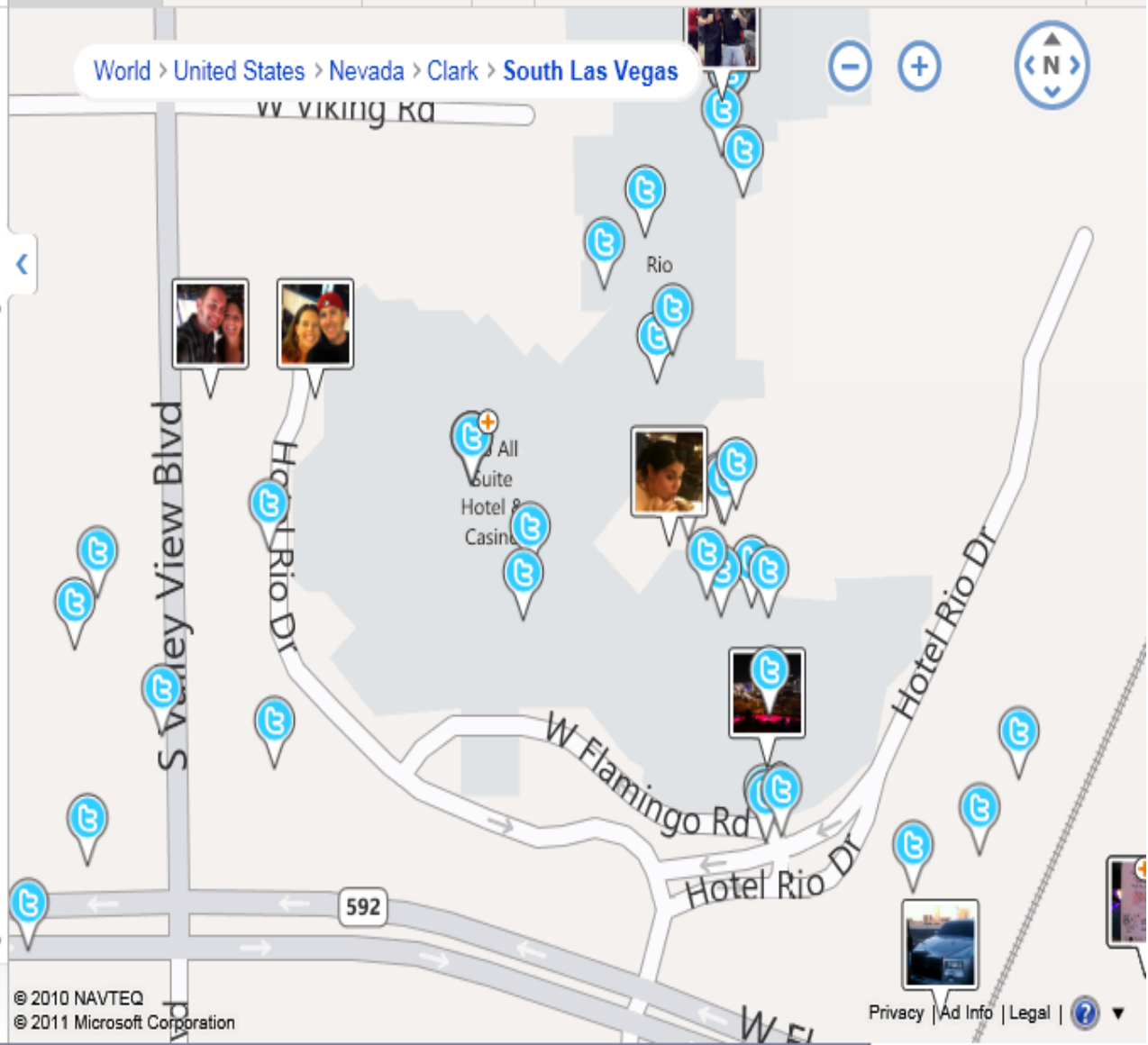
JuiicyGee

Marquee!!

about 18 hours ago from Twitter for iPhone

luesipher

Got the bottles in the ice... (@



- Follow us on Twitter
- Feedback & suggestions
- Embed in your site
- FAQs

Some Final Observations

WTF HAPPENED TO THE CONSTITUTION?

Unresolved questions

- Is email privacy protected by the Fourth Amendment? [**Warshak v. United States**]
- Is warrantless GPS tracking constitutional? [**United States v. Jones**]
- Can your cell phone be searched during a traffic stop? Is a warrant required to search it after an arrest? [**People v. Diaz**, CA and **State v. Smith**, OH]
- Can the government force you to reveal a password for an encrypted device? [**United States v. Fricosu**]

Is privacy dead?

- Perhaps not yet, but it's dying fast
- We can reclaim privacy by protecting our information and refusing to share so much voluntarily, and in turn increasing society's expectation of privacy
- Increase awareness by shining the light on governmental intrusions into privacy rights
- Shift our focus

A new focus

- Do you have the right to wear red hats on Wednesdays? Why or why not? Or should we ask the question another way?
- Enumerated powers, Ninth Amendment, Tenth Amendment, Fourteenth Amendment
- Islands of liberty in a sea of power, or islands of power in a sea of liberty?
- Only you can make a difference for you

Questions

WTF HAPPENED TO THE CONSTITUTION?

DEFCON

Sources and References

Assault on Privacy [http://assaultonprivacy.blogspot.com]

Criminal Procedure Flow Charts [http://www.scribd.com/doc/23861708/Crim-Pro-Flowcharts]

Search and Seizure Flowchart [http://jyates.myweb.uga.edu/CP_Midterm_Review.ppt]

Federal Court Rules That TSA 'Naked Scans' Are Constitutional [http://blogs.forbes.com/kashmirhill/2011/07/15/federal-court-rules-that-tsa-naked-scans-are-constitutional/]

The SWAT Team Would Like to See Your Alcohol Permit [http://reason.com/archives/2010/12/13/the-swat-team-would-like-to-se]

Minnesota Tenants Challenge Nosy Housing Inspectors [http://reason.com/blog/2010/12/29/minnesota-tenants-challenge-no]

National Security Letter [https://www.eff.org/files/filenode/ia_v_mukasey/Nov2007_NSL.pdf]

Twitter Unseal Order [http://www.salon.com/news/opinion/glenn_greenwald/2011/01/07/twitter/Twitter_Unsealing_Order.pdf]

DOJ's "hotwatch" real-time surveillance of credit card transactions [http://paranoia.dubfire.net/2010/12/dojs-hotwatch-real-time-surveillance-of.html]

Chicago's Video Surveillance Cameras Report [http://il.aclu.org/site/DocServer/Surveillance_Camera_Report1.pdf]

Supreme Court to Decide Constitutionality of Warrantless GPS Monitoring [http://www.wired.com/threatlevel/2011/06/warrantless-gps-monitoring-scotus/]

Using hidden cameras to catch car thieves [http://articles.baltimoresun.com/2011-06-22/news/bs-md-ho-trooper-death-license-reader20110525_1_license-plate-reader-car-thieves-motorcycle]

'Bong Hits 4 Jesus': Student Protest Goes to Supreme Court [http://abcnews.go.com/US/story?id=2953653&page=1]

Are Student Cell Phone Records Discoverable? [http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202503300012&slreturn=1&hbxlogin=1]

Texas 'Calorie Camera' Will Track How Much Students Eat [http://www.huffingtonpost.com/2011/05/11/texas-calorie-camera_n_860771.html]

School-Webcam Spy Scandal Resurfaces [http://www.wired.com/threatlevel/2011/06/webcam-scandal-resurfaces/]

Cell phone measure targets ID theft threat [http://www.pittsburghlive.com/x/pittsburghtrib/news/cityregion/s_509880.html]

U.S. Faces Legal Challenge to Internet-Domain Seizures [http://www.wired.com/threatlevel/2011/06/domain-seizure-challenge/]

Judge Who Doesn't Understand Technology Says WiFi Is Not A Radio Communication [http://www.techdirt.com/blog/wireless/articles/20110701/12225114934/judge-who-doesnt-understand-technology-says-wifi-is-not-radio-communication.shtml]

Note

- For the most up-to-date version of these slides, please visit [**http://www.scribd.com/theprez98**]


DEFCON
WTF Happened to the Constitution?!
The Right to Privacy in the Digital Age
Michael "theprez98" Schearer
DEFCON 19
Las Vegas, NV