

Your Mind: Legal Status, Rights and Securing Yourself

Tiffany Rad and James Arlen

Black Hat USA

July 29, 2009

We're going to make your brain hurt.

In a good way.

The hurt might even save your brain.

Disclaimer: Neither of us are speaking for our employers. We promise not to break the world.

Tiffany Strauchs Rad, MA, MBA, JD

- President of ELCnetworks, LLC.,
 - Business, tech and security consulting, legal services
- Part-time Adjunct Professor in the computer science department at the University of Southern Maine
 - computer law and ethics, information security
- Establishing a computer crimes clinic at Maine School of Law
- Organizer of HackME, a hacker space in Portland, Maine

James “Myrcurial” Arlen, CISA

- Part-time Security Consultant
 - Fortune 500, Profit 50, based in Toronto
- Part-time Chief Information Security Officer at a mid-sized financial
- Part-time stringer for Liquidmatrix Security Digest
- Full-time push-the-envelope next-gen super-duper visionary strategitarian
- Founder of think|haus, a hacker space in Hamilton, Ontario

Some definitions and legalese-to-english translations:

- Stored data and communications
- In-transit communications
- Legal person
- Legal adult
- Non compos mentis
- Common law
- Tort law
- Jurisdiction
- Agent (not secret, corporate)
- Contract

“Data” and “Document” are sometimes, but not always interchangeably used by lawyers and legislators.

We will use these working definitions:

- Data: the lowest level of abstraction from which information and knowledge are derived. IE: Bytes arranged in order.
- Document: a bounded physical representation of body of information designed with the capacity (and usually intent) to communicate.

Living Person (Person in Being) or Business Organization (Corporate Entity)?

- A company has some legal rights similar to a living person
 - A company can make contracts as well as sue and be sued
 - An Agent can “speak” for the business organization

Legal and Technical Differences:

- **Stored Communications**
 - When data has come to rest on a device
 - SCA derived from the ECPA
 - Lesser standard for warrants
- **In Transit Communication**
 - When data is still “moving” between devices
 - Higher standard for warrants

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.”

- Only works inside the borders of the USA
- Doesn't count *at* the border
- May be over-ridden by other laws and norms - USA PATRIOT ACT

Sanctity of your person is not absolute:

- T.S.A.
- Terry stop
- Warrant
- Third party permission to search

Sanctity of your “stuff” is even less absolute:

- Computers and compute devices
- Plain sight/view
- Non-related data
- Incomplete warrant

Warrants are applicable to external, small computing devices

- Cell phones
- PDAs
- Car Computers (in most states)
- Medical Devices

Fifth Amendment

“No person shall be held to answer for a capital, or otherwise infamous crime, unless on presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offense to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.”

- You cannot be forced to incriminate yourself
- No such right in Canada
- No such right at the border
- Other jurisdictions?

Consider the various ways in which the law treats data...

...For now, just keep in mind data which is stored in some way – not moving through networks.

Case One:

- Data stored in a cloud based application with servers in the USA
- IE: Google doc

- Search and seizure?
- By other governments?

- You are **PWN3D**

Case Two:

- Data stored in an external backup site with servers in the USA
- IE: Amazon S3

- Search and seizure?
- By other governments?

- You are **PWN3D**

Case Three:

- Data stored on a rented server with an ISP in the USA
- IE: Rackspace

- Search and seizure?
- By other governments?

- You are **PWN3D**

Case Four:

- Data stored on an owned server with an ISP in the USA
- IE: local colocation provider
- Search and seizure?
- By other governments?
- You are **PWN3D**

Case Five:

- Data stored on an owned fileserver located in your home in the USA
- Search and seizure?
- By other governments?
- You are **PWN3D**

Case Six:

- Data stored on an owned laptop that is kept in your personal possession in the USA
- Search and seizure?
- You are **PWN3D**

Case Seven:

- Data stored on a telecommunications device that is kept in your personal possession in the USA
- Search and seizure?
- You are **PWN3D**

Case Eight:

- Data stored on a data storage media that is kept in your personal possession in the USA
- Search and seizure?
- You are **PWN3D**

Don't be a fool – encrypt your data!

AES-1024 w/ 32768bit keys FTW!

...Ok – so what if you encrypt?

Obfuscated or Encoded (rot13, base64, etc)

- Commonly used as a legal 'defense' for DCMA
- Isn't going to save you.

Common off-the-shelf encryption

- Commercial options: PGP, Ironkey, others.
- Non-Commercial options: GPG, Truecrypt, etc.

- You'll give up the key.

Personal / self-developed encryption:

- One-time pad
- You are Bruce Schneier

- You'll give up the algorithm and the key.

All of the above refers to data at rest...

...What happens if the data is in motion?

Ok – that’s all great... you’re not making me feel better about my data, but I thought this talk was about my mind.

Lets just take a few minutes to tease apart what you mean when you talk about the difference between your stored data and your mind.

Before we launch in though – here’s a piece of historical case law to think about...

The contents of your desk/briefcase/valise – your “Personal Notes and Effects” have some protections...

How does that fall apart in this brave new world.

Where do you keep your memory?

Pretend it's still the '90s.

1990's PDA - "Assistant" -- names, addresses, phone numbers, relationships (PII of others), your PII+aspirations, future events, plans, etc.

Are we talking about "thoughts"/"memories" or personal notes and effects?

Are alarm settings legally an agent?

Pretend it's finally the early 00's.

Connected PDA – same as previous case but has some replicated data-stores.

The replicated copies are held by a corporation – is there an agency relationship?

Does the corporation have rights to your memory / knowledge?

What about when the memory is not ‘to remember something’ – but rather ‘to do some action’?

How about a cron job or scheduled task?

Google Search Alerts?

This is less about data and more about agency.

When we transition from “remember something” to “remember to do some action”... there’s a natural extension to:

“Make a decision for me.”

This is getting really close to the legal definition of agency.

We’re already doing this. My Outlook client decides whether or not to accept meeting invitations based on criteria that I give it.

Is there a bright line we can draw to distinguish your thoughts and memories from those you've recorded?

...At what point does the computer become a legal agent?

How am I related to my:

» Computer

- » hardware – chattel
- » software – explicit license with multiple corporations

» Data Storage

- » local - chattel
- » remote – contract with 3rd party

» Transmission Capability

- » direct – explicit license with the FCC
- » internet – contract with 3rd party

But is it even possible to “own” a computer in the sense that I can own a carrot?

If I’m not an owner but merely a licensee, who really owns my computer?

What the *&^#%!!!!!!

...but if the computer isn't "mine" in a reasonable sense, can it still make decisions that I am bound to?

...is there any other situation where a licensed non-entity can apparently enter into contracts on behalf of a natural person?

Do I have an explicit or implicit contract
with my computer?

Can a computer do these things and
somehow become legally “alive”?

What does it take to become "legally" an agent - for yourself or others?

Can we map out a "cognitive ladder" that one of these data/computer/information systems can climb towards legal maturity?

We already have a set of cases which describe the legal nature of less than adult. Are computer-based agents similar to children?

Various "adult" ages:

- » Age of Majority
- » Age of License
- » Age of Consent
- » Age of Criminal Responsibility

All of these vary from 7 - 21

There's quite a gap there in terms of capability or capacity for cognition.

The other obvious place where the law has considered the concept of cognitive maturity as it relates to legal maturity is in the case of mentally handicapped adults.

Could a computer pass these tests?

What happens when ELIZA meets Rainman.

Do these cognitive agents represent your thoughts?

If they do, they should have the same protections as your mind.

But if they don't...

What happens when...

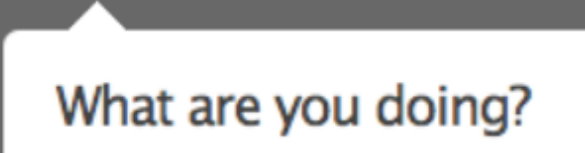
You can move actual memory out of your head and into a device.

You've probably already done this with some things...

- Do you keep track of phone numbers anymore?
- What about important dates?
- What are you doing next Thursday?

Let me just 'borrow' your phone – how's your memory now?

Record of your actions or activities...

The Twitter logo, consisting of the word "twitter" in its characteristic blue, rounded font, is displayed on a dark grey rectangular background.A white callout box with a pointer pointing to the Twitter logo, containing the text "What are you doing?".

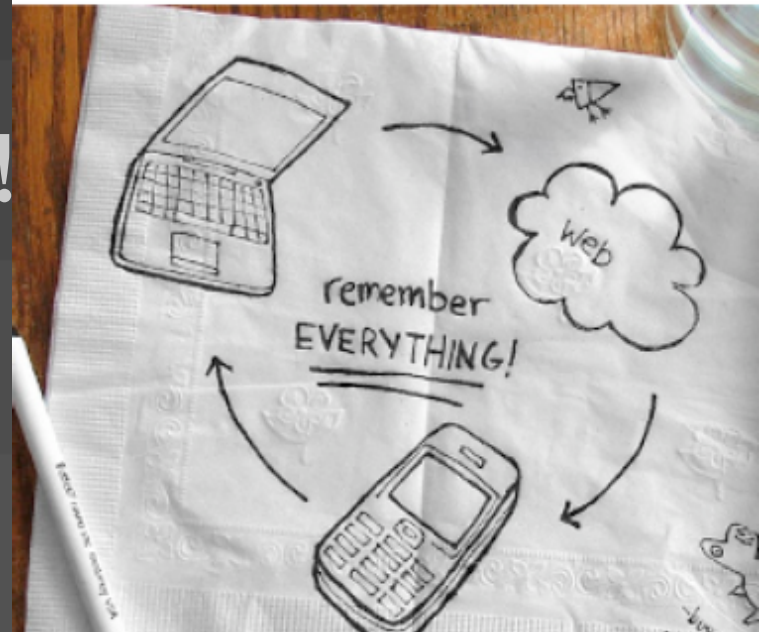
What are you doing?

- Are you establishing intent?
- Can you ever take it back?
- Your cell phone provider will turn over text messages – sometimes even without a subpoena.

But I'm a hipster and I want to have access to my memory everywhere –



I use Cloud Memory!!!



Who really controls your information?

Prosthetic Memory

The Microsoft Research SenseCam



Proven successful in aiding memory recall of Alzheimer's patients.

(image © Microsoft – from: <http://research.microsoft.com/en-us/um/cambridge/projects/sensecam/information.htm>)

...but you actively chose to use all of those things...

...you've done this to yourself...

...but what if you have no option?

Medical prosthetics are no longer “dumb” devices...

- Pacemakers
- Automatic Defibrillator (BH 2008-Kohno, Fu)
- Insulin / Drug Pumps
- Seizure Detection/Control

They include event loggers, wireless communications, and vulnerability to subpoena.

Public Surveillance beyond the simple CCTV

Future Attribute Screening Technology (FAST) assesses pre-crime thoughts.

FAST is grounded in research on human behavior and psychophysiology, focusing on new advances in behavioral/human-centered screening techniques. The aim is a prototypical mobile suite (FAST M2) that would be used to increase the accuracy and validity of identifying persons with malintent (the intent or desire to cause harm). Identified individuals would then be directed to secondary screening, which would be conducted by authorized personnel.

How the USA Dept. of Homeland Security views these things...

FAST
Future Attribute Screening Technology

Homeland Security
Concept and Technology

The scope of malintent includes a spectrum of potential scenarios.

The theory assumes several measures (cues) predict malintent.

FAST M2 is designed to detect malintent by combining these cues.

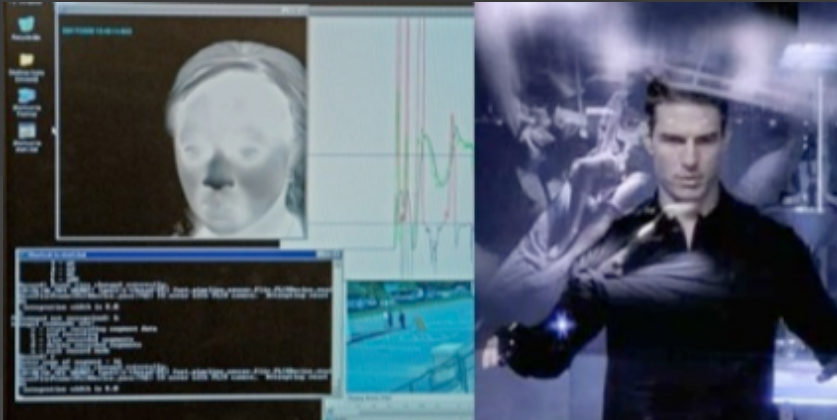
“After I get through I’ll cause a disturbance”
“After I get through I’ll detonate a bomb”
“After I get through I’ll deliver the package”

Nonverbal Behavioral Cues (Body movements, illustrating gestures, etc.)
Paralinguistic Cues (Vocal effects)
Psychophysiological Cues (Physical responses to emotional reactions)

Heart Rate
Respiration
Pupil Dilation
Thermal Signals
Additional Cues
CLARIFY

CLARIFY

Detailed description: This is a presentation slide for FAST (Future Attribute Screening Technology) by the US Department of Homeland Security. The slide is divided into three main sections. The top section features the title 'FAST Future Attribute Screening Technology' and the DHS logo. The first section, titled 'The scope of malintent includes a spectrum of potential scenarios,' shows a person at a security checkpoint with three speech bubbles containing phrases like 'After I get through I'll cause a disturbance'. The second section, 'The theory assumes several measures (cues) predict malintent,' illustrates a person walking through a checkpoint with callouts for 'Nonverbal Behavioral Cues', 'Paralinguistic Cues', and 'Psychophysiological Cues'. The third section, 'FAST M2 is designed to detect malintent by combining these cues,' shows a person at a 'CLARIFY' station with a diagram of various physiological and behavioral cues being analyzed. The diagram includes boxes for Heart Rate, Respiration, Pupil Dilation, Thermal Signals, and Additional Cues, all pointing to a central 'CLARIFY' hub. A person is shown interacting with the station, which has a 'CLARIFY' sign on its side.



...Are your thoughts legible at a distance?

...Are you ok with a blanket grant on what you might be thinking?

...How do you control your biometry data once it's measured and taken by others?

Employers collecting biometric data on employees – what does it reveal about your thoughts?

- FBI is collecting biometric data stored in the Clarksburg, West Virginia facility



RFID + Security: Don't Mess With Las Vegas?

Third Eye has a new RF-based security system, SATS (Security Alert Tracking System) based on a wristband biosensor (from SPO Medical) that monitors employee's heart rate.

If the rate suddenly increases, management is alerted by an RF signal from the wristband.

The premise is that if a casino employee's heart starts suddenly beating rapidly, they are likely under stress. This could be due to some emergency such as a robbery, or possibly because the employee is planning a theft.

<http://www.rfidgazette.org/security/>

...Where is the boundary between thoughts that are private and thoughts that are available in the public realm?

Is the man with the magic box stealing my soul?

...So my thoughts can be made public and can be used against me. At least that's out of my control.

...What if my thoughts conspire against me?

...It's not like there's ever been software written that had a flaw...

...and bad people like to exploit flaws in computer software, and wouldn't mind knowing what I'm thinking about...

...and since my computer is legally an agent and can make binding decisions - even contracts on my behalf...

...or the government could retroactively declare some thought or memory as illegal and prosecute me for it...

...thanks for scaring the crap outta me...

What can be done?

How can I protect myself?

James: IANALJASD

- I am not a lawyer, just a security dude.

Tiffany: IAALBNYL

- I am a lawyer, but not your lawyer.

NOTE: If you follow this advice,
you're likely safer, but you
can be screwed anyways.

Practical measures for keeping your thoughts safe while they are stored.

- Keep them in your home.
- Use encryption.
- Don't give any cause to make them look hard.
Truecrypt hidden partitions are findable.
- Store data in difficult to subpoena places.
- Launch your own datastorage satellite.

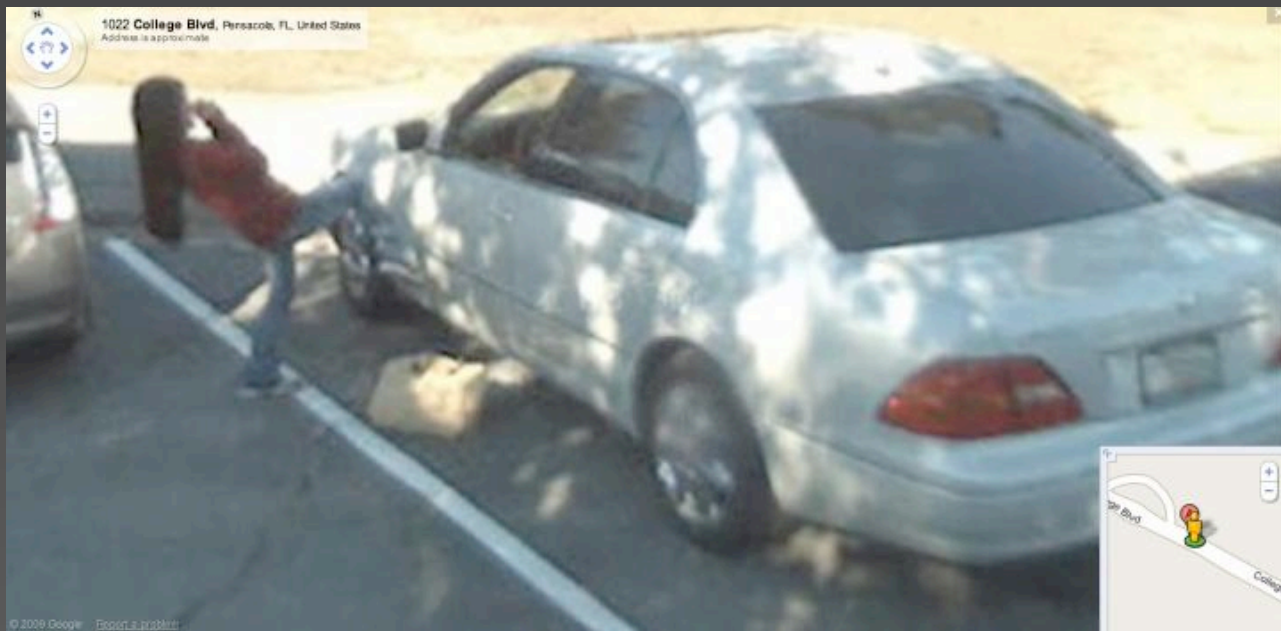
Practical measures for managing newly forming cognitive agents.

- Beware licensing.
- Limit capability.
- Resist the urge to join the digerati.
- Work to maintain and improve digital civil liberty and privacy legislation

The best advice is simple awareness that
your mind and your memory
isn't necessarily your own.

In conclusion, we're asking you to do your part to engage with the general public, legislators and vendors. Help them to understand that we may not need entirely new ways of dealing with what we're creating, but we **MUST** consider the implications prior to unleashing our new overlords.

» If you're inspired by Carrie Underwood's *Before He Cheats*, don't get caught doing it on camera...



» Or if you happen to be in range of a FAST camera, don't act stupid and think peaceful thoughts...



» ...or go into a data base forever with the caption “...There can be only one!” associated with your image and legal name



Q & A

followup:
tiffany@elcnetworks.com
myrcurial@100percentgeek.net

Thanks and Notices

Tiffany Strauchs Rad

Links:

<http://www.tiffanyrad.com>
<http://www.tiffanyrad.blogspot.com>

White paper with references on
Tiffanyrad.com

Thanks: My family, Hackerspaces crew, and
Black Hat organizers.

Inspirations: Nothingface, hackerish
children, EFF, Bard Coffee (Portland,
Maine), European techno, and my
University of Southern Maine students.

James “Myrcurial” Arlen

Links:

<http://myrcurial.com> and
<http://www.linkedin.com/in/jamesarlen>
and sometimes
<http://liquidmatrix.org/blog>

Thanks: My Family, Friends, and
Black Hat organizers.

Inspiration: my lovely wife and hackerish
children, Coffee, Strattera, Club
Mate, Information Society, NIN,
altruism.

Constructed with: Apple Macbook Pro,
Firefox, Powerpoint, angst.



<http://creativecommons.org/licenses/by-nc-sa/2.5/ca/>

2009-07-29

Your Mind: Legal Status, Rights and Securing Yourself -- Blackhat USA 2009