

**THE ROAD LESS
SURREPTITIOUSLY
TRAVELED**

@pukingmonkey

DEF CON 21

THE LOSS OF LOCATIONAL PRIVACY WHILE TRAVELING IN YOUR AUTOMOBILE

- Automatic License Plate Readers (ALPRs)**
- Snitch devices in your car**
 - Transponder based Electronic Toll Collection (ETC)**
 - GPS**
 - Smart phones traffic apps**
 - Dumb phones**
 - Automatic tire pressure monitors**

DO YOU HAVE THE RIGHT TO TRAVEL?

Interstate: YES. Saenz v. Roe (1999) the right to travel that is guaranteed by the Privileges or Immunities Clause of the Fourteenth Amendment.

Intrastate: YES. But not as clear, it's usually derived from First Amendment freedom of association and Fifth Amendment due process protection.

International: YES. Kent v. Dulles (1958) The right to travel is a part of the "liberty" of which a citizen cannot be deprived without due process of law under the Fifth Amendment.

DO YOU HAVE THE RIGHT TO DRIVE?

NO

It is a privilege, not a right, that is regulated, must be granted (licensed) and can be revoked, according to the prevailing laws of every jurisdiction of the United States.

DO YOU HAVE THE RIGHT TO ANONYMOUS TRAVEL?

Mostly **YES** but it depends on your mode of travel, in the U.S. you are not required to carry ID except:

- when driving, it requires licensing **NO**
- taking a commercial flight **NO**
- crossing a national border **NO**

AUTOMATIC LICENSE PLATE READERS

A system of cameras, computers and GPS that reads the license plates (OCR), and notes coordinates and time, they can be mobile or fixed locations.

Can do about 3,000 plates/hour, on moving vehicles up to 130MPH.

All data is saved and downloaded to a central repository.

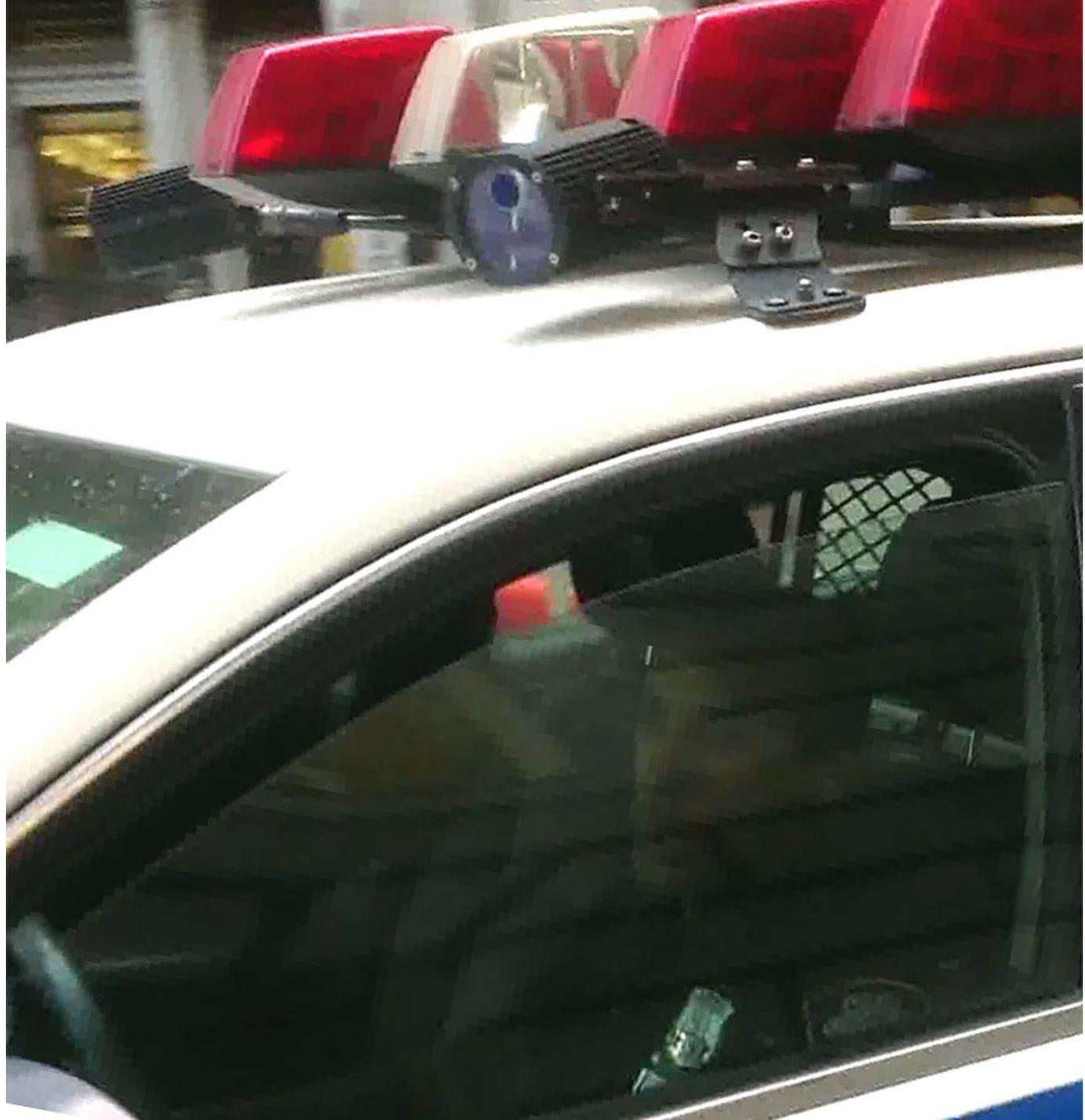
Some ALPRs



















**NOT ALPRs
(nor red light cam)**



NOT ALPRs (red light cam)



WHAT'S THE BIG DEAL?

Police have been “running” plates forever

- **Captures all plates in its field of vision**
- **retained in databases along with pictures from 21 days to 5 years (depends on jurisdiction)**
- **Enough APLRs and data points = tracked
NYC: 108 fixed and 130 mobile APLRs as of 2009**
- **Impossible to opt-out**

IS IT LEGAL TO DO THIS WARRENTLESS TRACKING?

YES

- **Hester v. United States (1924)** An observation made by a police officer without a physical intrusion into a constitutionally protected area does not implicate the Fourth Amendment nor require a search warrant.
- **United States v. Martin (1986)** A police officer who is lawfully present in an area may look into the windows of a parked car.
- **No reasonable expectation of privacy on your license plate in public**
- **Police do not need a warrant to "run" your plate**

**WAIT A MINUTE THE SUPREME
COURT RULED A WARRENT IS NEEDED
FOR GPS TRACKING**

YES BUT THIS IS DIFFERENT

**United States v. Jones (2012) what the court
said is that a warrant is needed to place the
tracking device on the vehicle, not the act of
tracking it.**

I THOUGHT THE POLICE CANNOT USE ADVANCED SPY TECHNOLOGY WITHOUT A WARRENT

YES AND NO

- **Kyllo v. United States (2001)** infrared **cannot** be used to look inside a constitutionally protected area
- **Florida v. Riley (1989)** aerial surveillance **can** be used
- **United States v. Lee (1927)** artificial illumination **can** be used to aid observations
- **binoculars can** be used (no Supreme Court case but Scalia has said it is OK)

FEMA AS BEEN FUNDING LOCAL PDS 100% OF THE COST OF ALPRs

 <p>Department of Homeland Security FEMA Grant Programs Directorate</p>	<p>Grant</p>		<p>PAGE 1 OF 2</p>
<p>I. RECIPIENT NAME AND ADDRESS (Including Zip Code) Vermont Department of Public Safety 103 South Main Street Waterbury, VT 05671-2101</p>	<p>4. AWARD NUMBER: 2009-SS-T9-0075</p>		
<p>1A. GRANTEE IRS/VENDOR NO. 036000274</p>	<p>5. PROJECT PERIOD: FROM 08/01/2009 TO 07/31/2012 BUDGET PERIOD: FROM 08/01/2009 TO 07/31/2012</p>		
<p>3. PROJECT TITLE PY 09 Homeland Security Grant Program</p>	<p>6. AWARD DATE 08/21/2009</p>	<p>7. ACTION Initial</p>	
<p>12. SPECIAL CONDITIONS THE ABOVE GRANT PROJECT IS APPROVED SUBJECT TO SUCH CONDITIONS OR LIMITATIONS AS ARE SET FORTH ON THE ATTACHED PAGE(S).</p>	<p>8. SUPPLEMENT NUMBER 00</p>		
<p>13. STATUTORY AUTHORITY FOR GRANT</p>	<p>9. PREVIOUS AWARD AMOUNT</p>		<p>\$ 0</p>
	<p>10. AMOUNT OF THIS AWARD</p>		<p>\$ 6,651,545</p>
	<p>11. TOTAL AWARD</p>		<p>\$ 6,651,545</p>



VERMONT DEPARTMENT OF PUBLIC SAFETY

State of Vermont
Standard Grant Agreement

Agreement #02140-79252-005

Parties: This is a Grant Agreement between the State of Vermont, **Department of Public Safety** (hereinafter called "State"), and **city of Burlington Treasurer / Burlington Police Department** with principal place of business at **1 North Avenue, Burlington, VT 05401** hereinafter called "Subrecipient").
Subrecipient is/ is not required by law to have a Business Account Number from the Vermont Department of Taxes. The Account Number is # _____.

Subrecipient Federal Tax Identification Number: 03-6000410
Subrecipient DUNS Number: 614816635
Subrecipient Full Physical Address as provided on the CCR Registry (PO Box not acceptable):
1 North Avenue, Burlington, VT 05401

Subject Matter: The subject matter of this Grant Agreement is State Homeland Security Grant-Equipment. Detailed services to be provided by the Subrecipient are described in Attachment A.

Grant Term: The period of Subrecipient's performance shall begin on June 14, 2011 and end on December 31, 2011. "The State will not reimburse any expenses incurred prior to the execution date of this agreement. The execution date is defined as the date the Department of Public Safety representative(s) signs this agreement"

Maximum Amount: In consideration of the services to be performed by Subrecipient, the State agrees to pay Subrecipient, in accordance with the payment provisions specified in Attachment B, a sum not to exceed \$22,460.00

Source of Funds: Federal Funds 100 %
Match required: Yes No If Yes: \$ N/A

<u>CFDA Title</u>	<u>State Homeland Security Grant Program</u>
<u>CFDA Number</u>	<u>97.067</u>
<u>Award Name</u>	<u>FY 09 Homeland Security Grant Program;</u>
<u>Award Number</u>	<u>2009-SS-T9-0075;</u>
<u>Award Year</u>	<u>2009;</u>
<u>Federal Granting Agency</u>	<u>U. S. Department of Homeland Security;</u>
<u>Research and Development Grant?</u>	Yes <input type="checkbox"/> No <input checked="" type="checkbox"/>

Amendment: No changes, modifications, or amendments in the terms and conditions of this Grant Agreement shall be effective unless reduced to writing, numbered, and signed by the duly authorized representative of the State and Subrecipient.

Cancellation: This Grant Agreement may be suspended or cancelled by either party by giving written notice at least 30 days in advance.

Contact persons: The Subrecipient's contact person for this award is: Andi Higbee, Deputy Chief
Telephone Number: 802-540-2111 E-mail address: ahigbee@bpdvt.org

ELSAG North America Law Enforcement Systems, LLC

412 Clocktower Commons
 Brewster, NY 10509
 Duns # 196140821
 Phone: 1-866-9MPH900 (967-4900)
 Fax: 336-379-7164

DATE

5/3/2011
****QUOTATION****

Delivered to:

Burlington Police Dept.
 Att: Lt. Jennifer Morrison
 1 North Ave.
 Burlington, Vermont 05401

Quotation valid until: August 31, 2011

Prepared by: Pat Fox

Projected Arrival Date: TBD

(Please mail your PO to the address above or FAX copies to the number above and also FAX a copy to (518) 452-7777.

Receipt of Goods

NASPO Multi-State Contract #PC62119 Award #19745
 (California Participating Addendum)
WSCA # PC 62119 Hazardous Incident Response Equipment
 (Contract term: September 2, 2005 - May 31, 2015)

Model #	Description	Cost	Units	Amount
MPH-900X2AD3 SPLIT TRANS	Mobile License Plate Reader - Includes two units with LPR Processors, camera (color and IR LPR); Infrared illuminators, enclosures, junction box, cables and related software. (REQUIRES INSTALLATION BY AUTHORIZED ELSAG N.A. PERSONNEL)	\$16,350	2	\$32,700.00
MPH-900 INSTALL	IN A TRANSPORTABLE RUGGEDIZED CASE. Hedley mounts with a CLICKER to be mounted on a Ford Crown Victoria's.			
OPERATION CENTER LICENSE	Operations Center License	\$975	2	\$1,950.00
ADDITIONAL CAR KIT	1 extra power cord (\$125.00), 1 extra ethernet cable (\$100.00) and 1 extra GPS unit with USB extension (\$110.00) for a Total of \$335.00 to power up an additional vehicle.	\$335	2	\$670.00
EXTENDED WARRANTY	3 yr. extended warranty @ \$1,600.00 per year times 3 yrs. For a Total of \$4,800.00 per LPR unit times 2 units for a Total of \$9,600.00.	\$9,600		\$9,600.00
			TOTAL	\$49,920.00

Service Plan for goods and services provided by the above quote

Year	Cost	Includes
Year I	Free	
Year II	\$1,600.00 per year per LPR unit	Hardware and Software
Year III	\$1,600.00 per year per LPR unit	Hardware and Software
Year IV	\$1,600.00 per year per LPR unit	Hardware and Software

Service Plan Includes:

- Software Updates
- Annual Training/Service
- Parts & Labor

Approval Signature: _____



ALPR DATA RETENTION

- **NH: general ban**
- **ME: 21 day maximum for non-hit non-criminal investigations**
- **NJ: must retain for a full 5 years, and then must destroy after 5 years**
- **NYC: retained for 5 years.** Even though general surveillance video is deleted after 21 days if no active investigation

IS THE DATA PUBLIC OR OPEN TO LEGAL DISCOVERY?

- Public? Maybe. Minneapolis released then recanted. GPS coordinates for their fixed readers was redacted.
- Discovery? NY has what is known as Rosario material, “Any written or recorded statement...made by such witness...which relates to the subject matter of the witness’s testimony.” However NY claims that ALPR data is not a "statement" so therefore it is not Rosario, and not subject to discovery.

ACTUAL LPR DATA (MOBILE UNIT)



BOSS3

10/22/2012 10:48:58

Read Details

William Palmer



MANUAL ENTRIES

MPDMDC6SQ2387 - Unit 995

186CMR

10/7/2012 10:50:19

44.9782

-93.2631



From Hotlist =

186CMR

10/7/2012 10:30:32

44.9782

-93.2632



From Hotlist =

186CMR

10/7/2012 10:16:50

44.9776

-93.2626



From Hotlist =

186CMR

8/14/2012 15:09:52

44.9777

-93.2626



From Hotlist =

Total Reads for MPDMDC6SQ2387 - Unit 995 = 4

ACTUAL LPR DATA (FIXED REDACTED, THEN MOBILE)



BOSS3

12/11/2012 10:07:28

Read Details

William Palmer



[REDACTED]

[REDACTED]

SKA189

10/2/2012 19:08:52

[REDACTED]

From Hotlist =

Total Reads for [REDACTED] = 1

Total Reads for [REDACTED] = 1

MANUAL ENTRIES

MPDMDC3MD2448

SKA189

11/30/2012 11:17:44

44.9772

-93.2664



From Hotlist =

SKA189

9/17/2012 08:37:57

44.9771

-93.2664



From Hotlist =

Total Reads for MPDMDC3MD2448 = 2

IT MAY NOT MATTER WHAT RETENTION LAWS ARE, AS THERE IS A COMMERCIAL MARKET

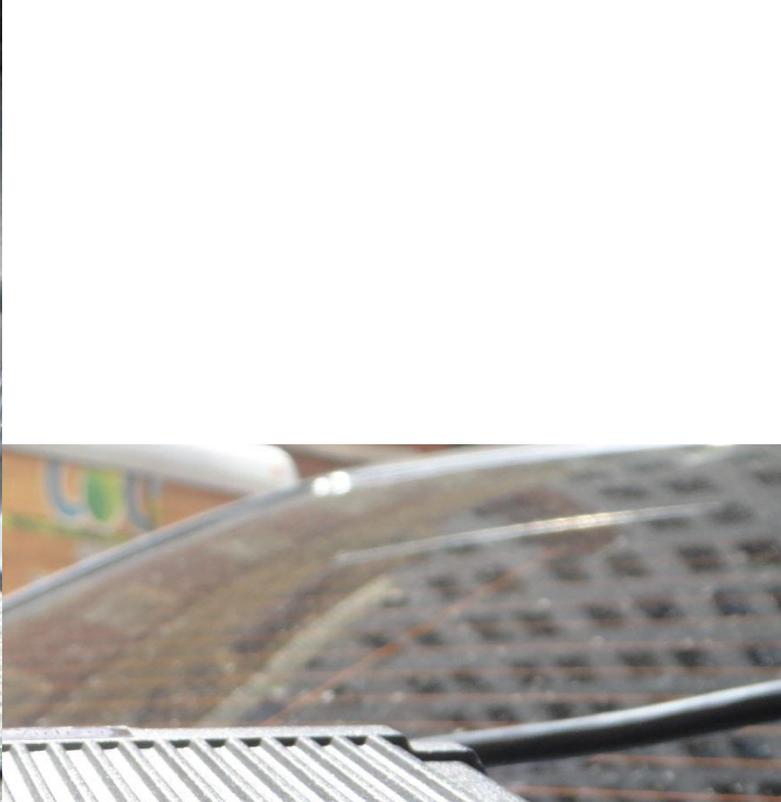
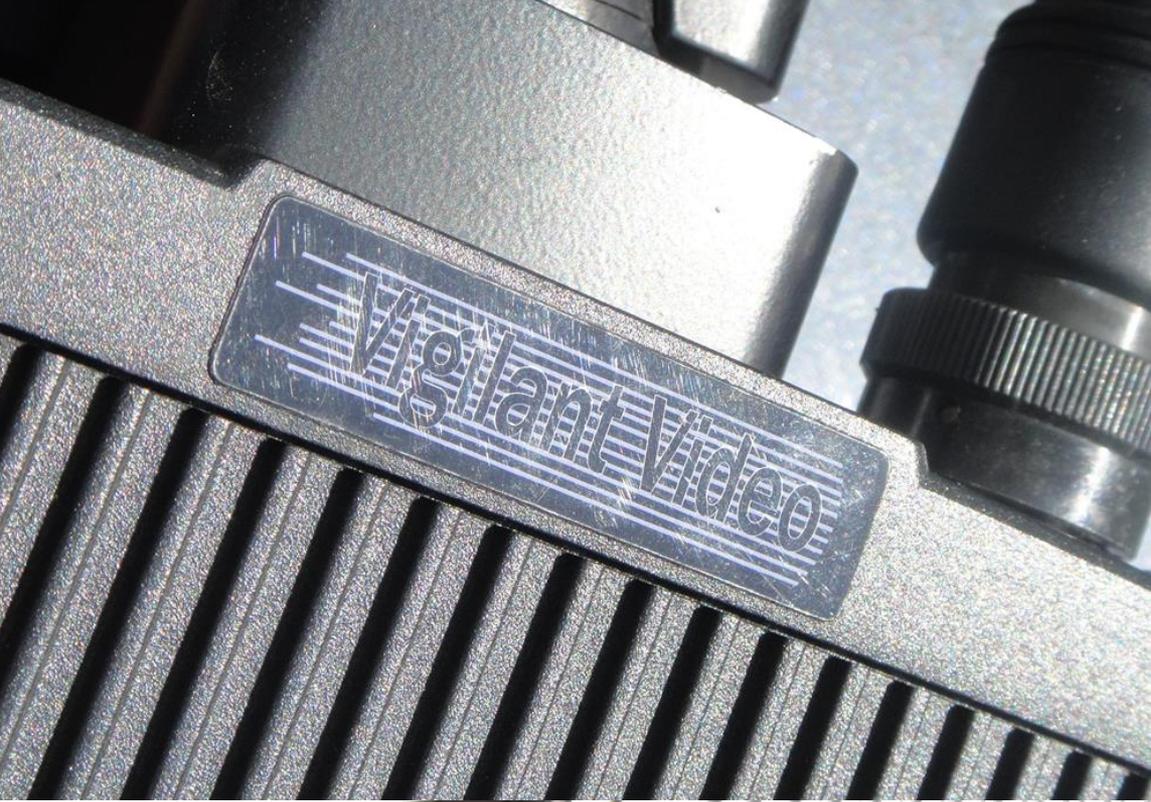
- **Vigilant Solutions.** it's only customers are Law Enforcement. Its in 28 Metro areas, >35 million reads/month, collected by non-law enforcement scout cars
- **Tow operators driving and scanning everything, looking for repo hits, but then sell the data.**
- **Law Enforcement will just purchase the data**



IMPALA

FLEXFUEL
E85 + ETHANOL

NEW YORK
FWF-6071
EMPIRE



BUILD A LICENCE PLATE READER DETECTOR

- **It uses infrared LEDs to illuminate the plate**
- **Its always on, and it is always pulsating to try to get the best exposure**
- **So we should be able to detect, by just using IR photodiodes right?**
- **Had a few failures to work**
- **Standard IR is 850nm. ELSAGs unit uses 735nm LEDS which near-IR (or far-red)**

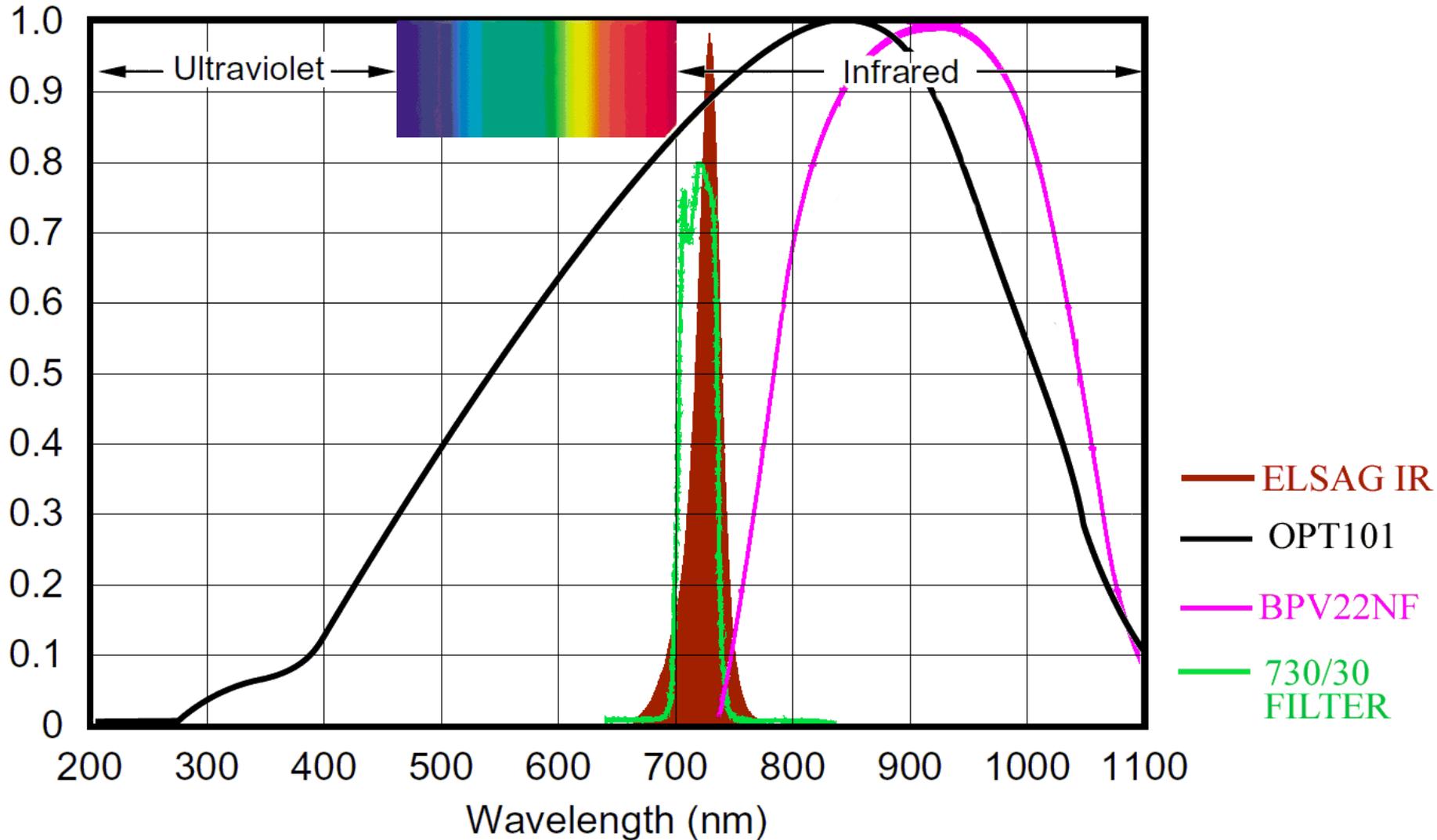
720nm IR PASS



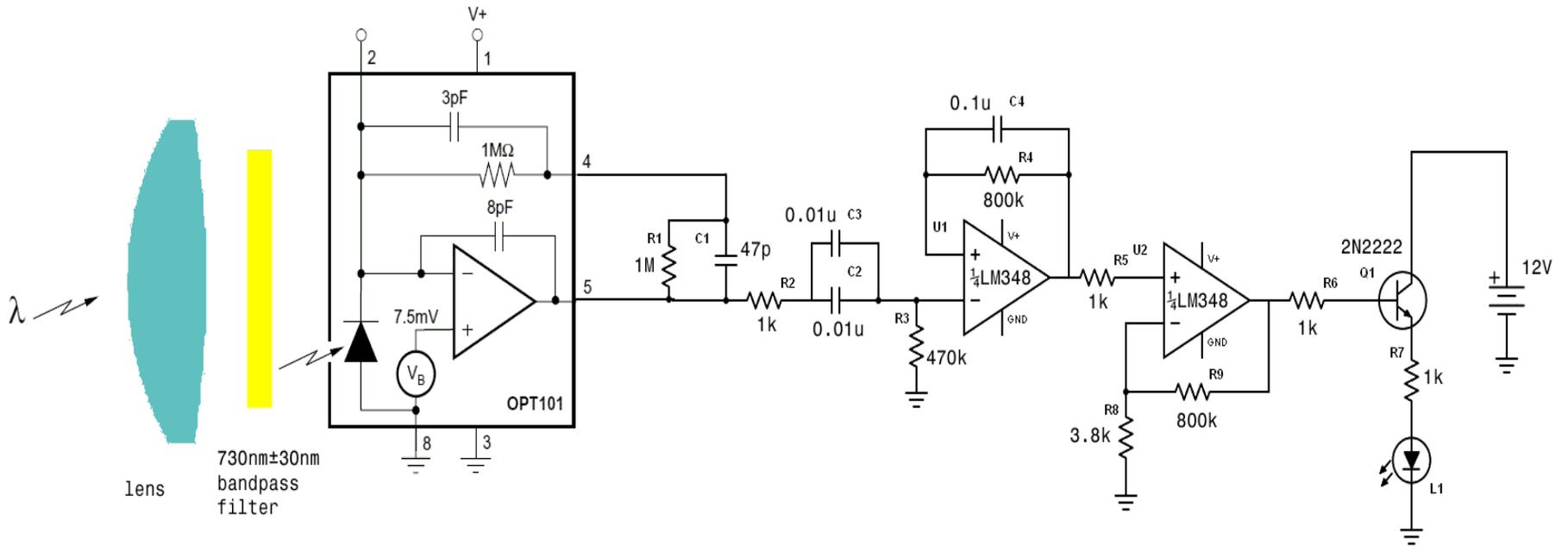
730±30nm BANDPASS

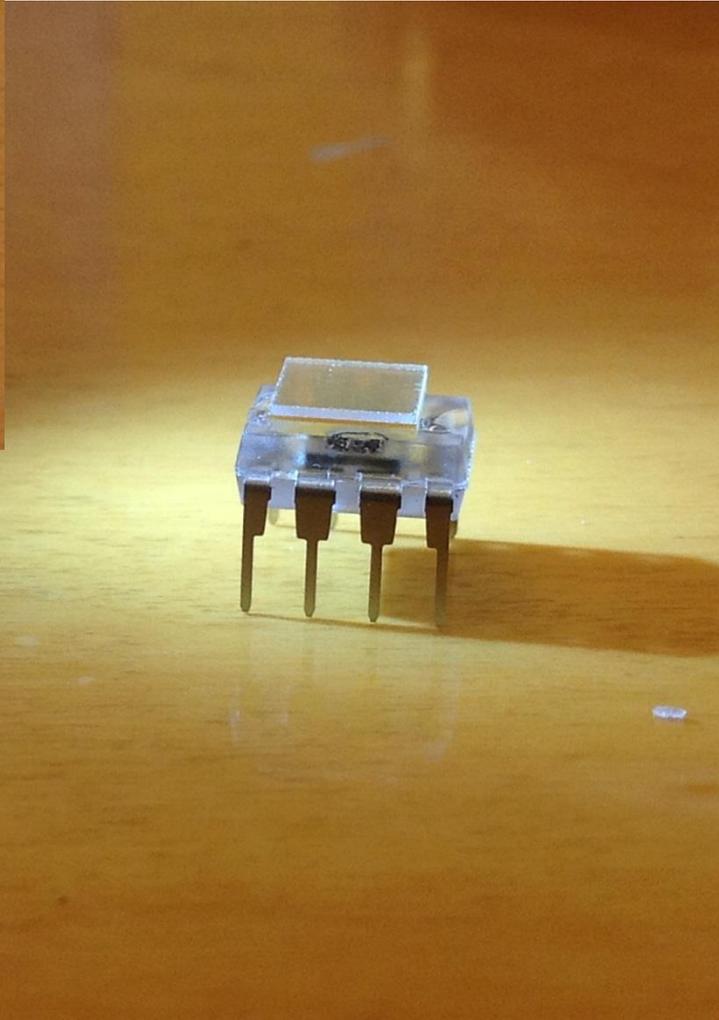
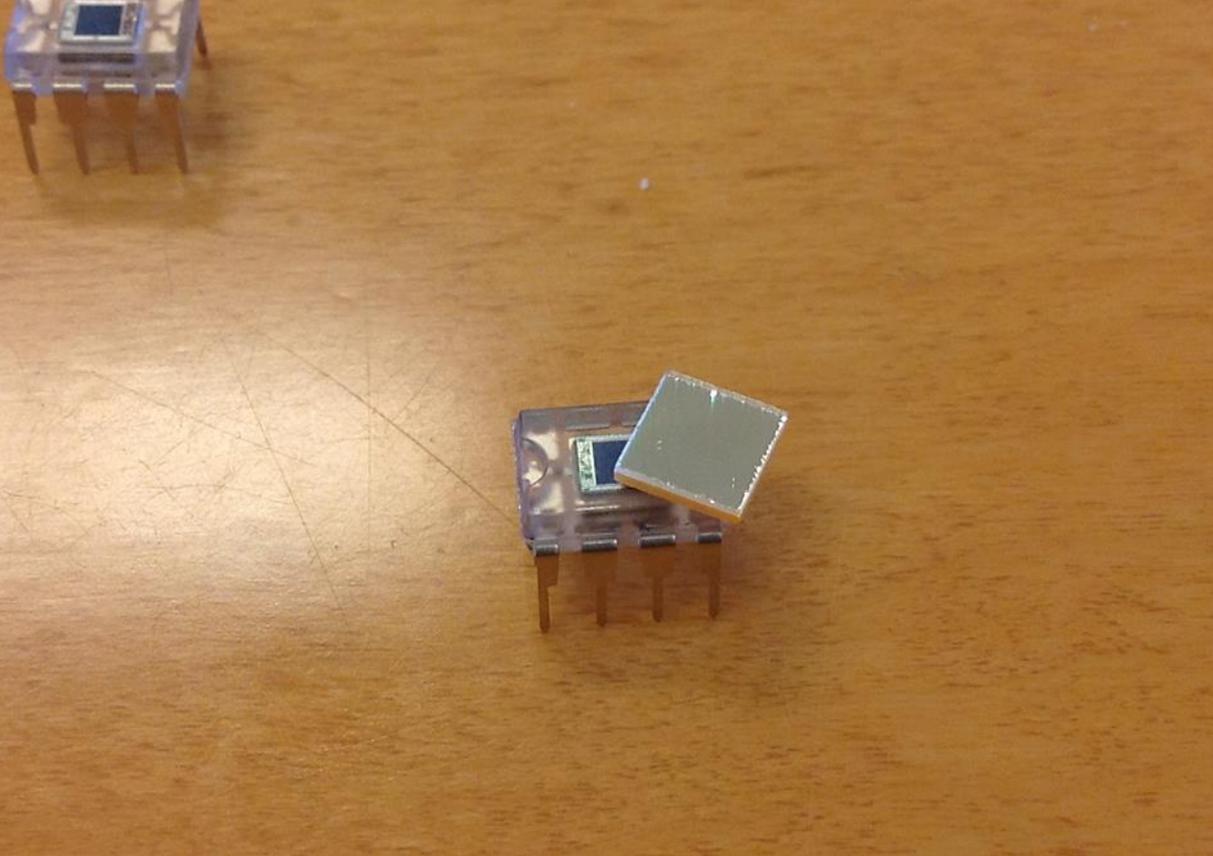


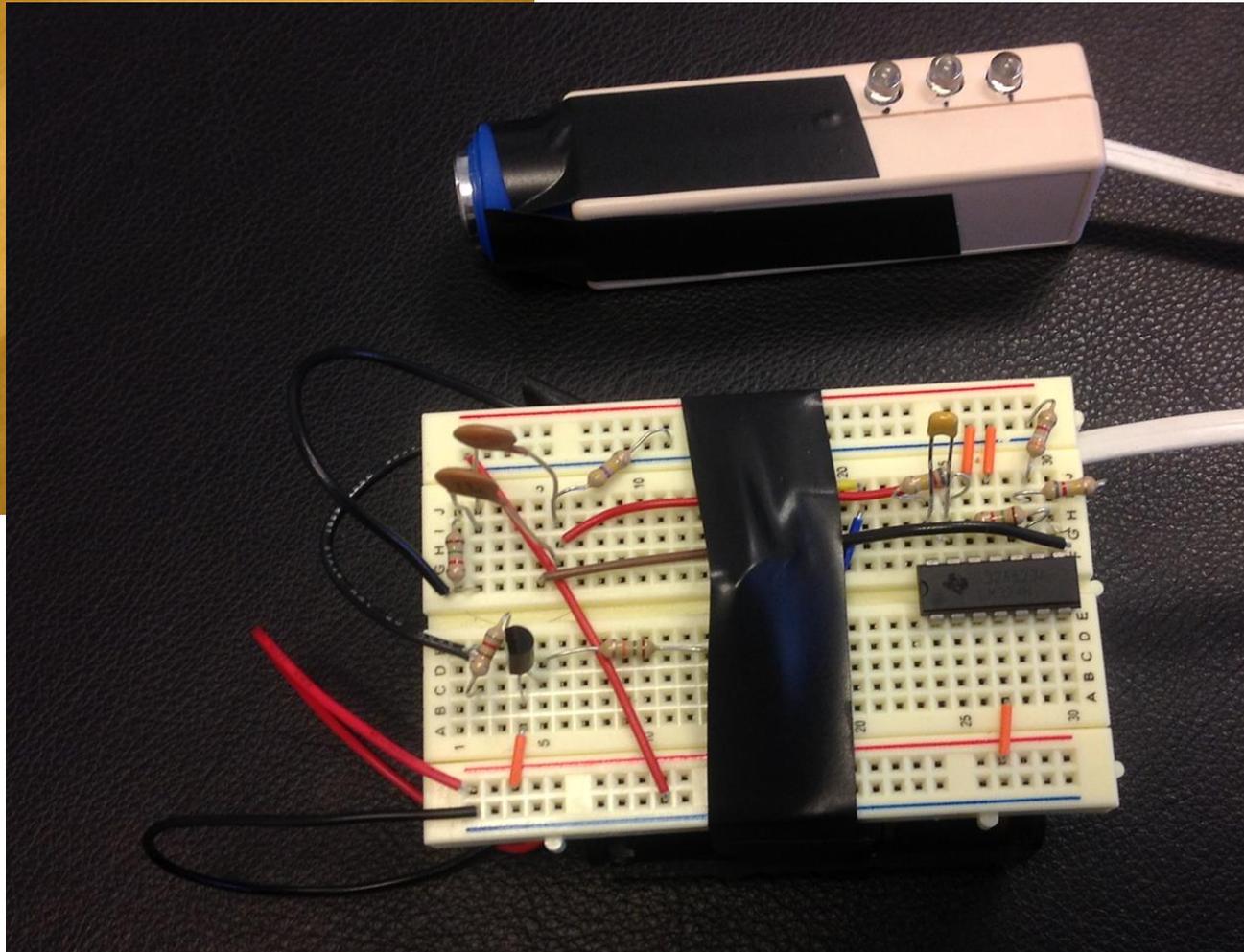
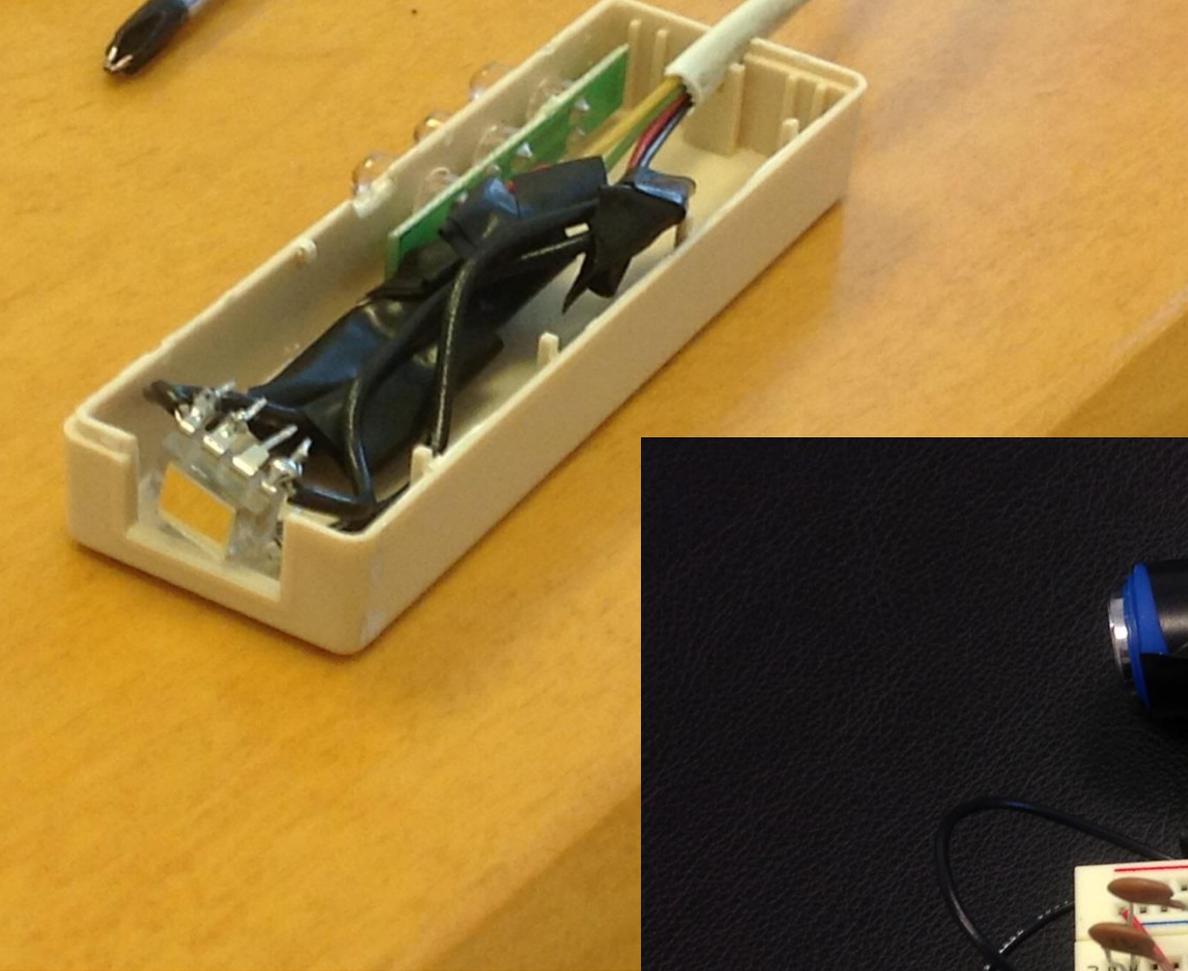
WHY STANDARD IR PHOTODIODES WON'T WORK



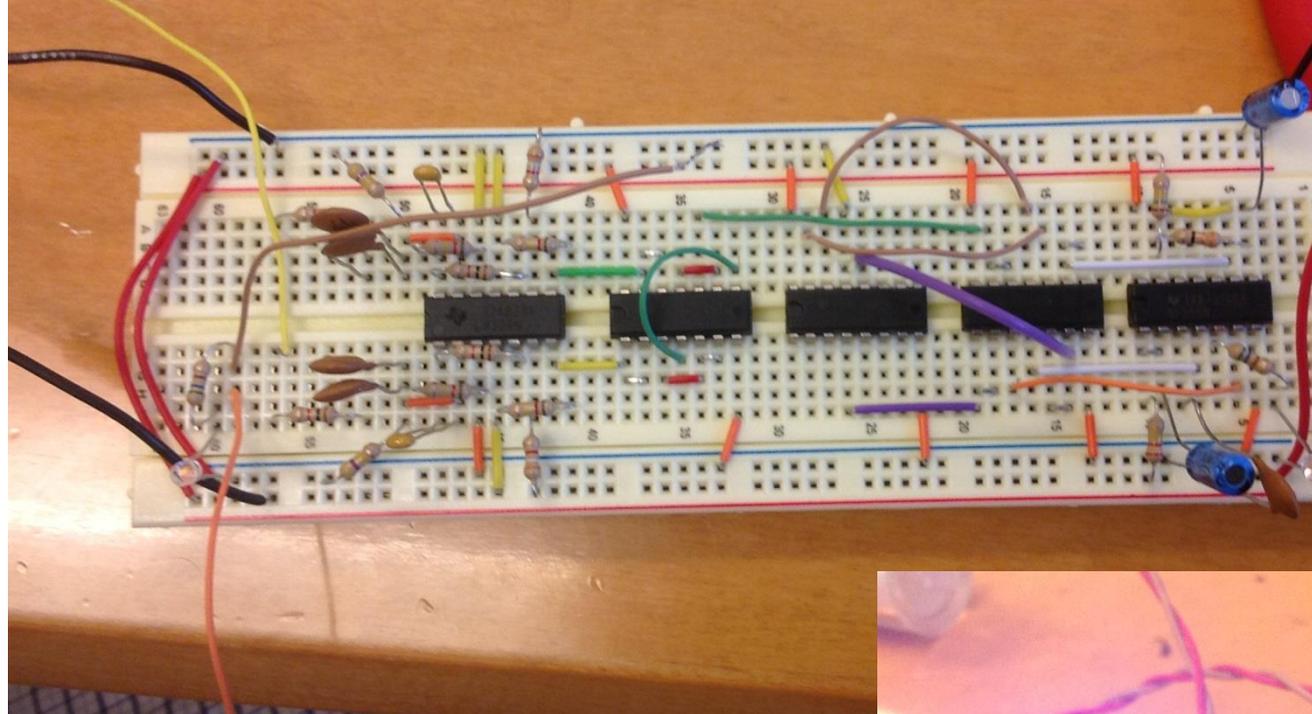
Working basic ELSAG Circuit







**It eventually
turned into
this. The
monkey
screams
When it
detects
an ALPR**



WHAT TO DO?

Well Steve Jobs never had plates



MAYBE LAW ENFORCEMENT CAN HELP









Drive with the tail gate down?

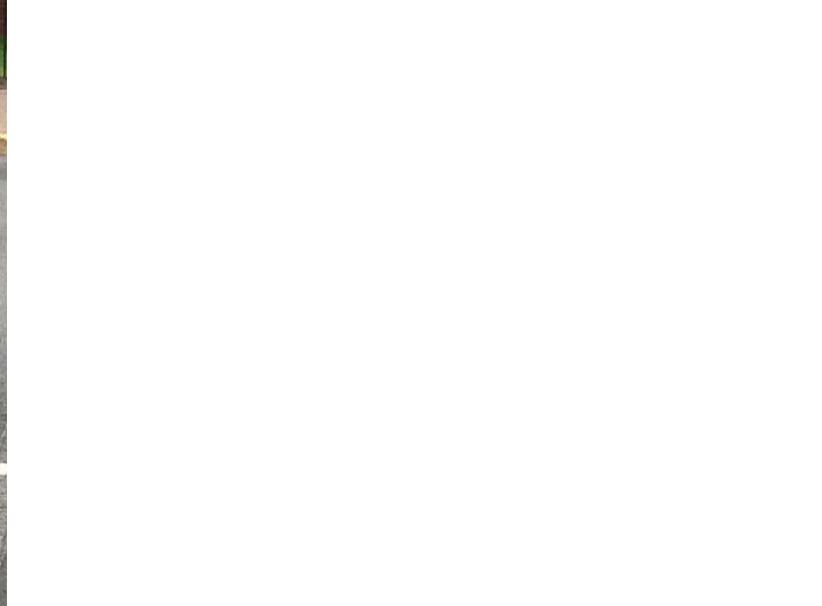




Yep seems to be a thing, different day



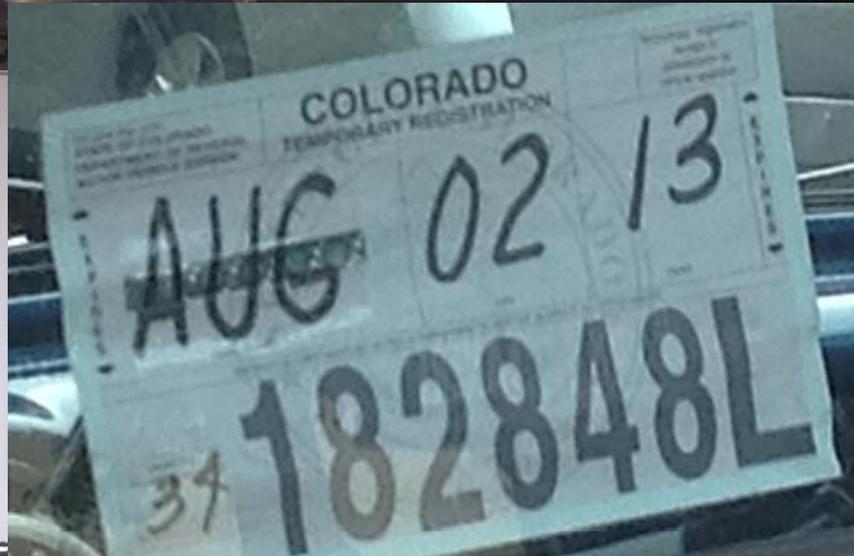




WHAT DO COPS DO?

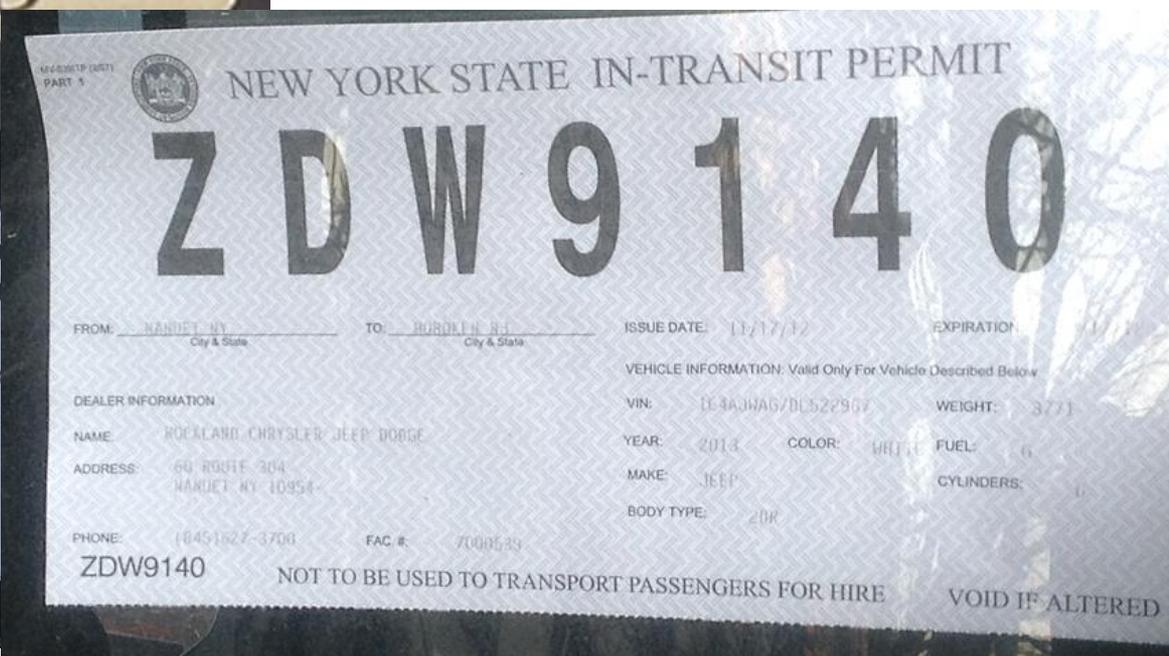
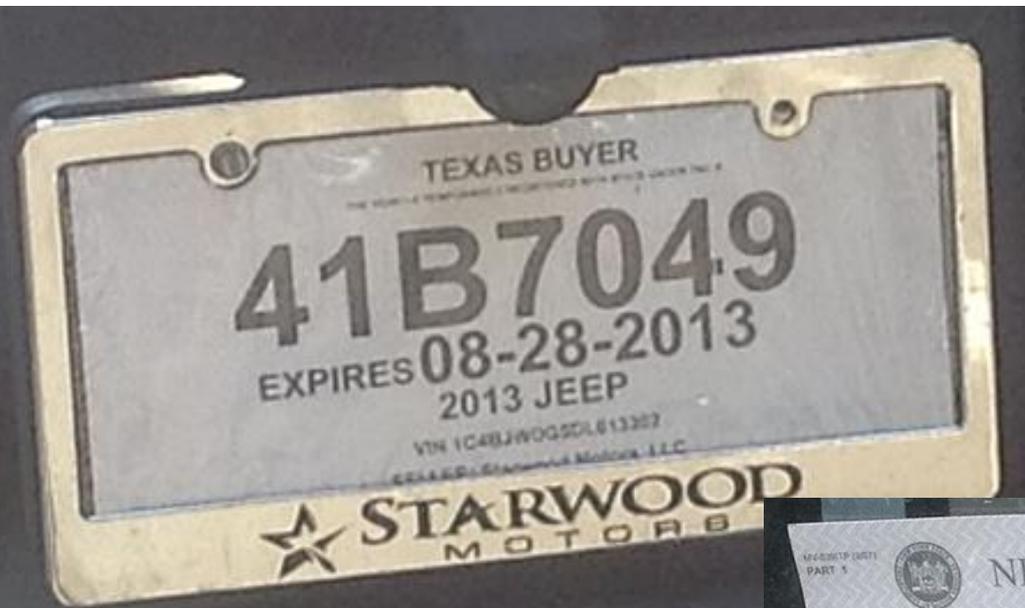
- **No front plate, even if required**
- **Heavily mask the back plate with dark plastic or alternating Fresnel lenses**
- **Drive with the tail gate down**
- **Also tint you windows and windshield....**
- **You CANNOT do any of this legally**
- **Don't want any extra interaction with law enforcement**

TEMP TAGS



TEMP TAGS

**BE WARNED THAT NY
TEMP TAGS ARE NOT
HONORED IN MA, CAR
WILL BE IMPOUNDED**



WHAT ARE THESE?

No number
VIN and
Expiration date

How do we get
them?

**TEMPORARY PLATE
LEASED COMMERCIAL FLEET VEHICLE**

PLATE ID#: _____

BL#: **3365254**

YEAR#: 2013

MAKE#: Dodge

MODEL#: Grand Caravan VIN#: **2C4RDGBG1DR586542**

MONTH DAY YEAR
02 24 13

(DATE LISTED IS 30 DAYS FROM ISSUE DATE - REGISTRATION REQUIRED 30 DAYS FROM ISSUE DATE)

AMERIFLEET

© 2006 AmeriFleet Transportation, Inc. ALTERATIONS VOID THIS PLATE

**GEORGIA TEMPORARY PLATE
LEASED COMMERCIAL FLEET VEHICLE**

PLATE ID#: No 259634

BL: **3358914**

YEAR: **2013**

MAKE: **FORD**

MODEL: **Transit**

MONTH DAY YEAR
02 16 13

(DATE LISTED IS 30 DAYS FROM ISSUE DATE - REGISTRATION REQUIRED 30 DAYS FROM ISSUE DATE)

VIN #: **NM0LS6AN2DT130688**

AMERIFLEET

© 2006 AmeriFleet Transportation, Inc. ALTERATIONS VOID THIS PLATE

- **CA you can drive a new car with no tags for 90 days (was 6 months while Jobs was alive) and cannot drive outside of CA**
- **Most temp tags are only good 20 to 90 days**
- **Registering you vehicle to a company hides you in a thin veil, but still plates are recorded**
- **But do NOT get commercial tags**

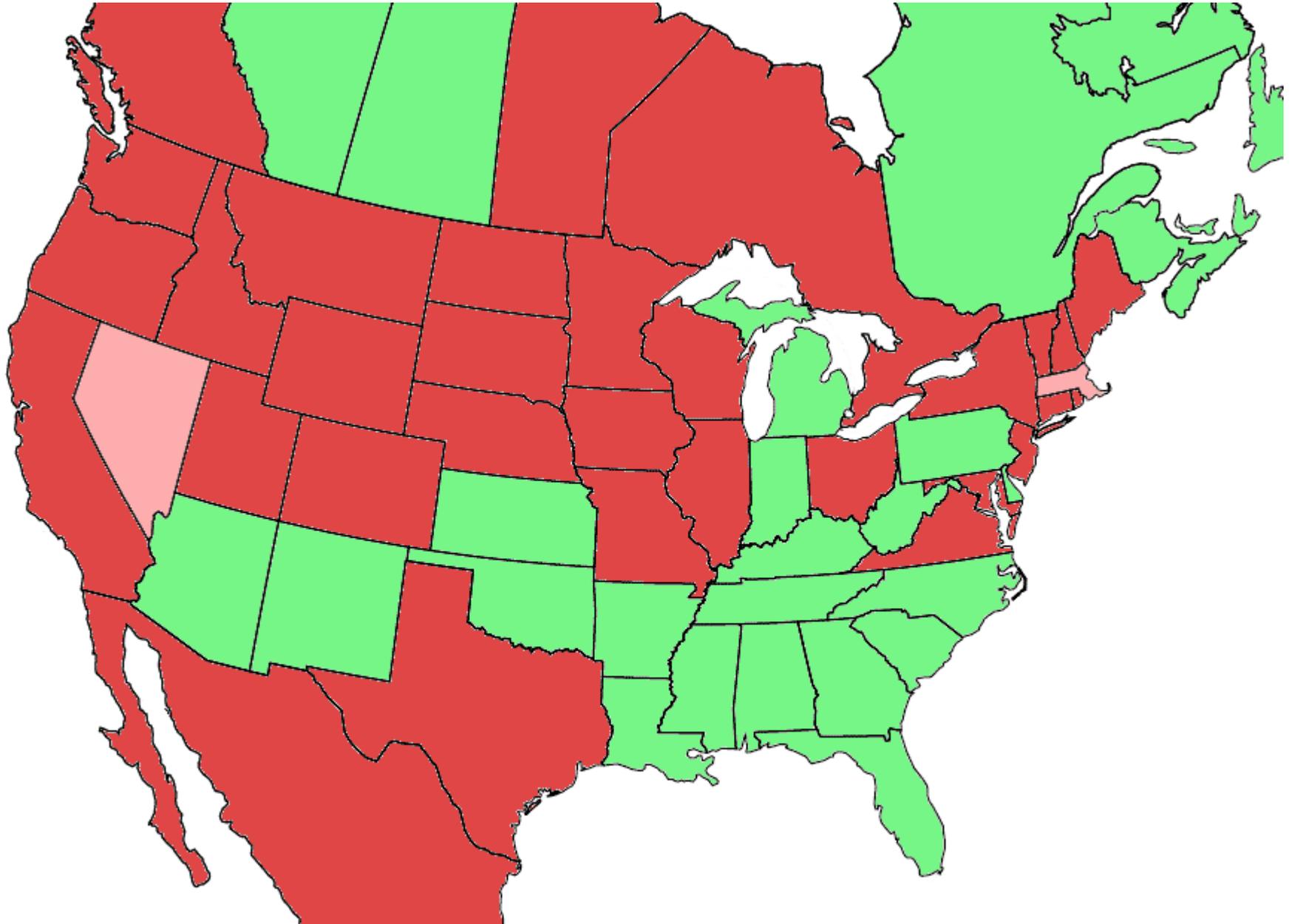
PERILS OF COMMERCIAL PLATES



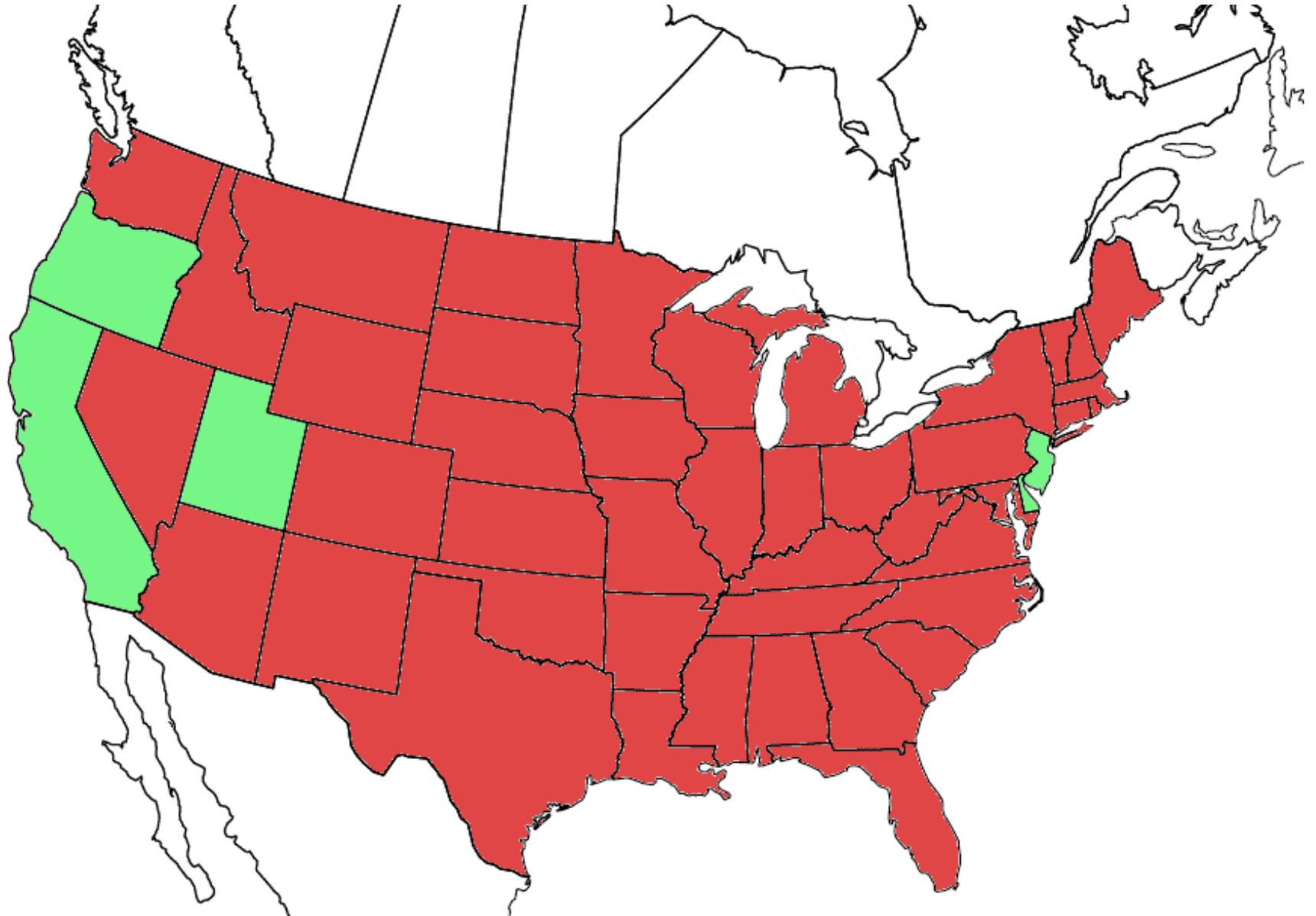
WHAT IS HARDEST FOR ALPR

- **Non reflective plates**
 - **Crime to remove reflectivity in CA**
 - **Failed inspection in MA if you plate loses reflectivity**
- **Low contrast plates**
- **Light red characters**
- **With 3 or more stacked letters**
- **Registration stickers that need to be placed close to the letters**
- **8 digit plates, smaller and narrower letters**
- **Also no front plate, means half the chance of being read**

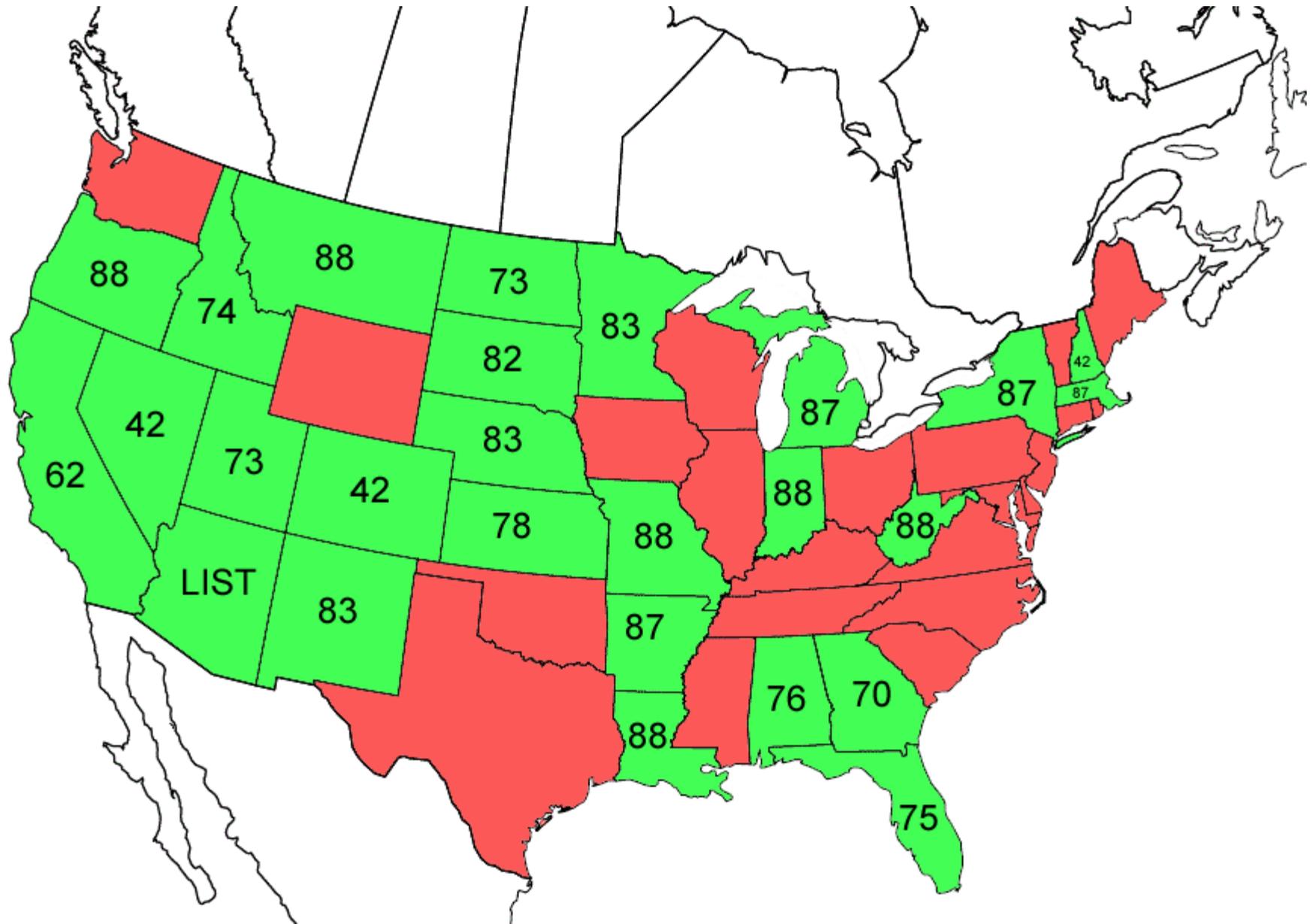
ONE VS. TWO PLATES



STATES WITH LEGAL NON-REFLECTIVE PLATES



LATEST MODEL YEAR FOR YOM



OBSCURED PLATE





**OBSCURED
PLATES**





**“M” is not part of the plate number
(with stacked letters)**



BUMPER GUARDS



BUMPER GUARDS

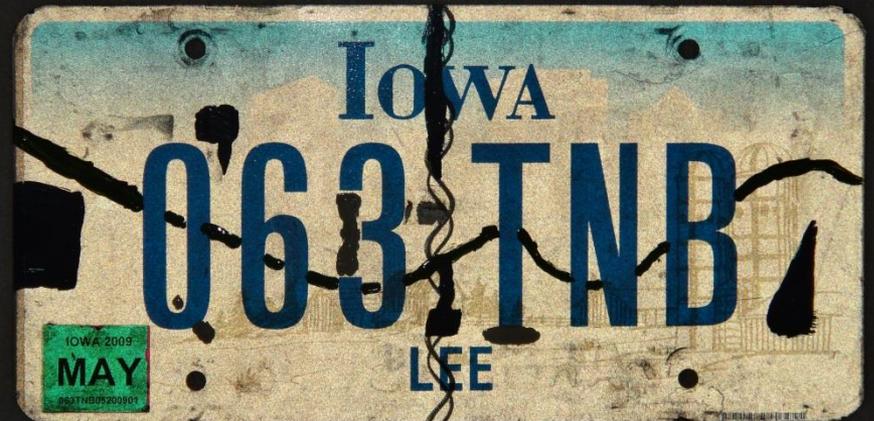


LEGALLY OBSCURED FRONT PLATES

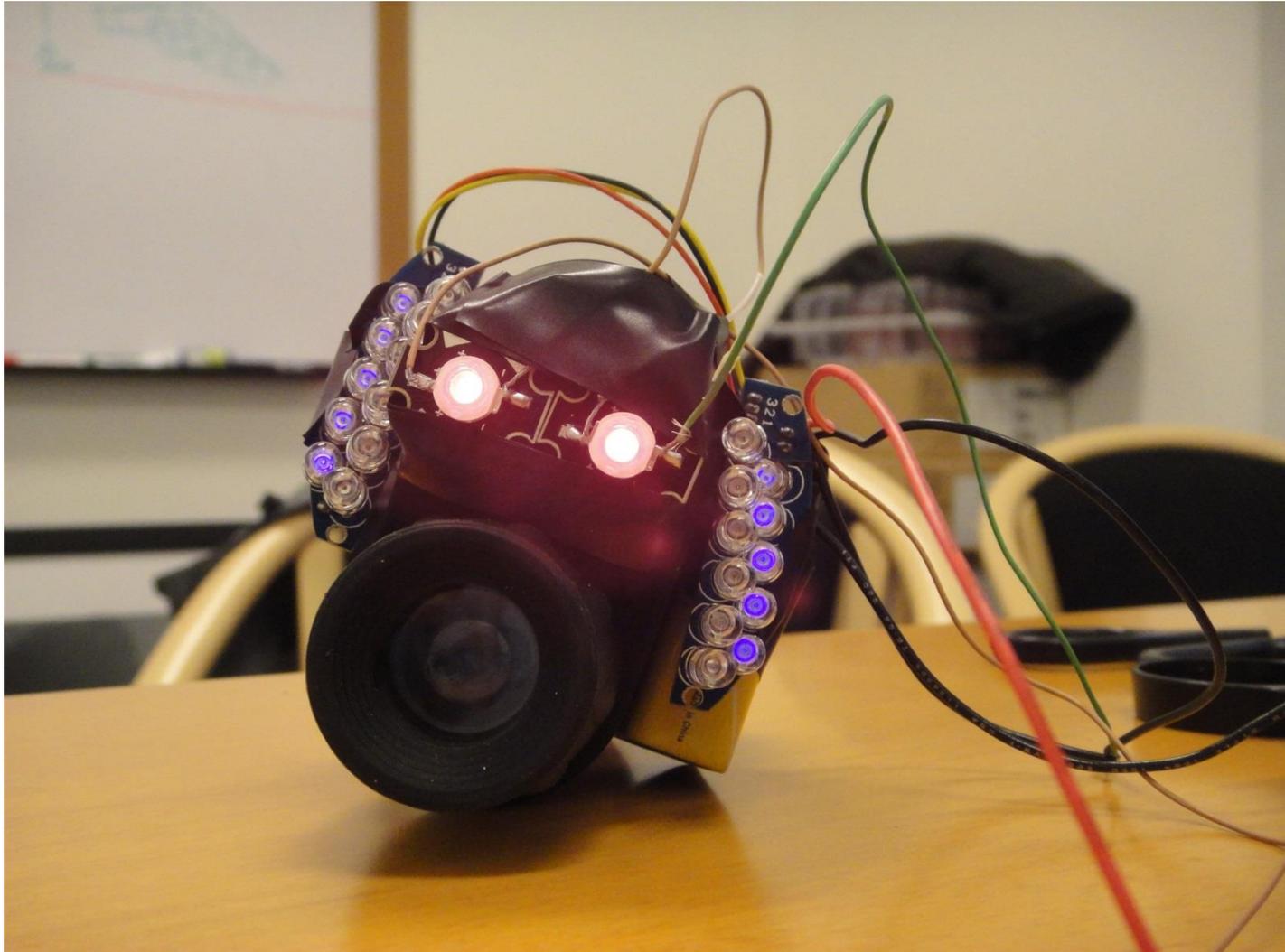


CAPTCHA PLATE

- NO! DO NOT DO THIS, IT IS DOCUMENTS



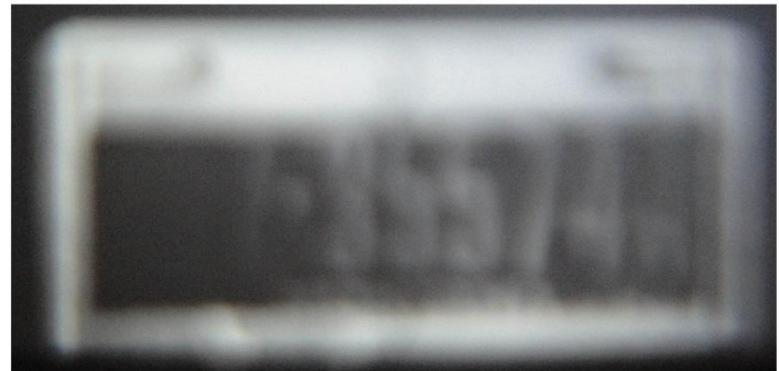
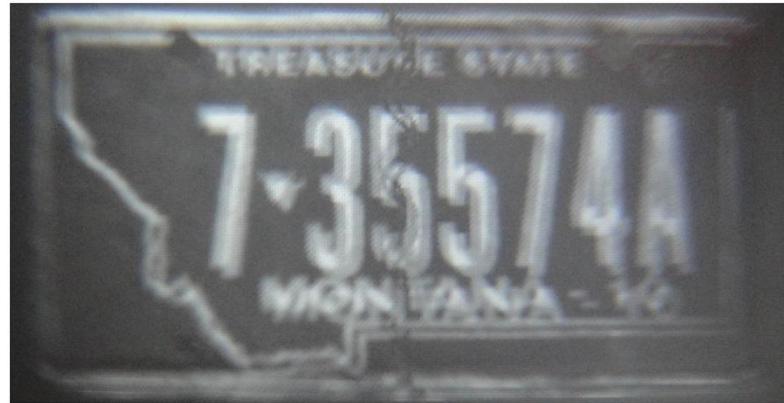
IR CAMERA WITH 735nm AND 850nm



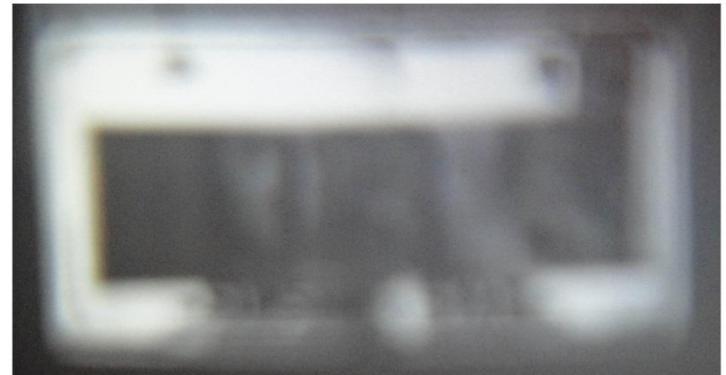
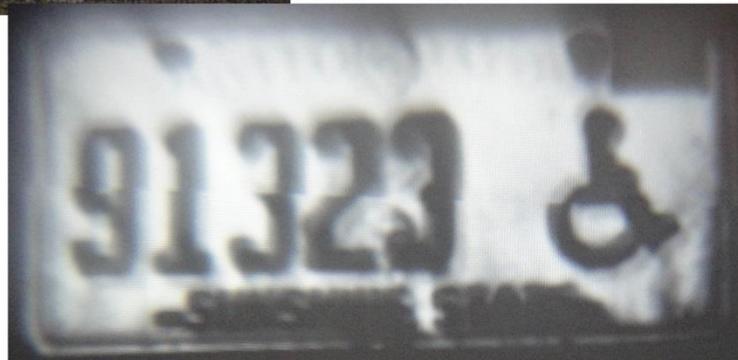
VISIBLE, IR VIEW, WITH IR BLOCK 850nm



VISIBLE, IR VIEW, WITH IR BLOCK 850nm



VISIBLE, IR VIEW, WITH IR BLOCK 850nm



LIGHTLY SALTED PLATE

VISIBILE, FLASH, IR 735nm

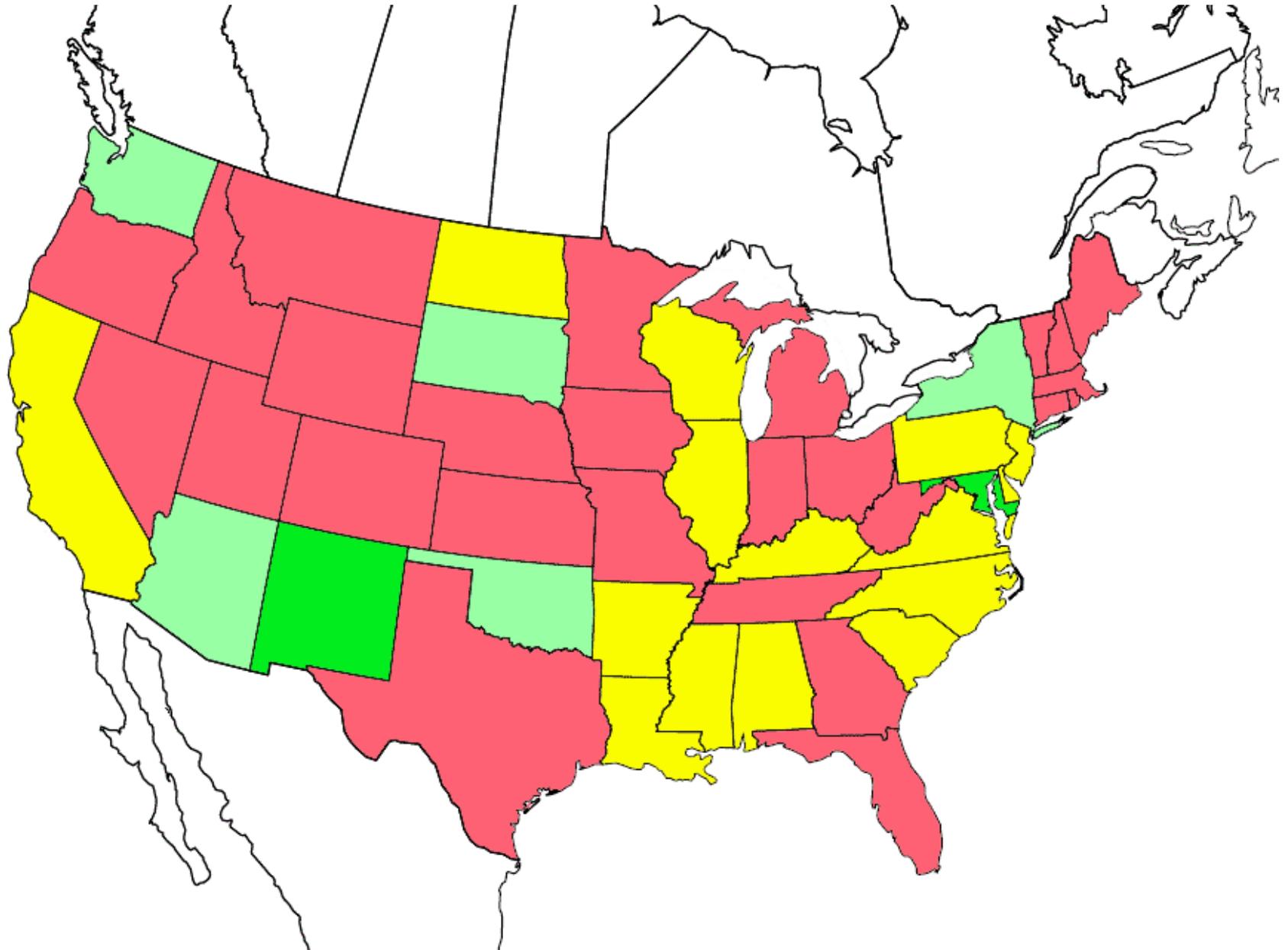


HEAVILY SALTED PLATE

VISIBILE, FLASH, IR 735nm



NUMBER OF STACKED CHARACTERS



NY (good) vs NJ (no good) 3 STACK



STATES WITH SPECIAL CHARACTERS

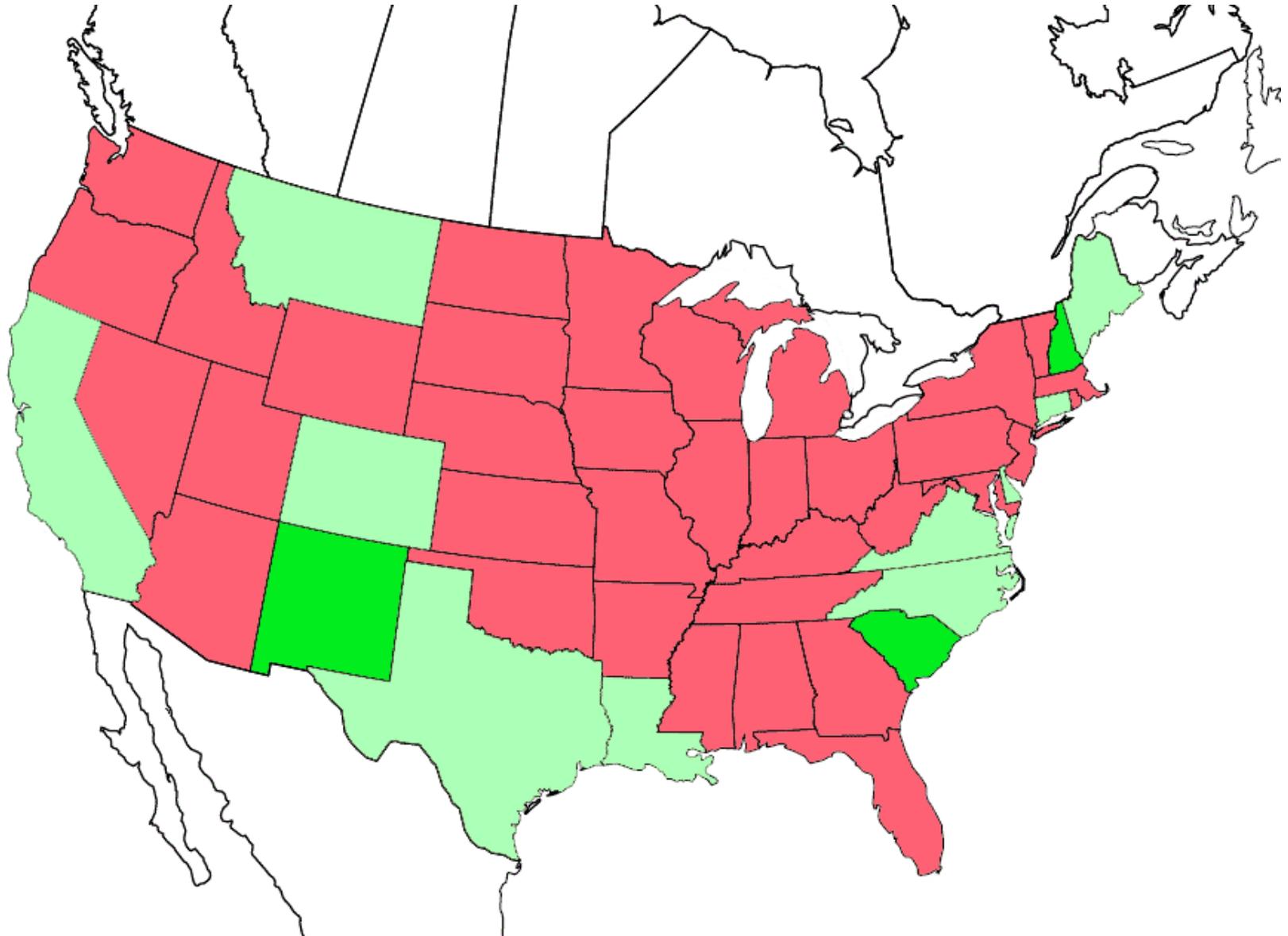
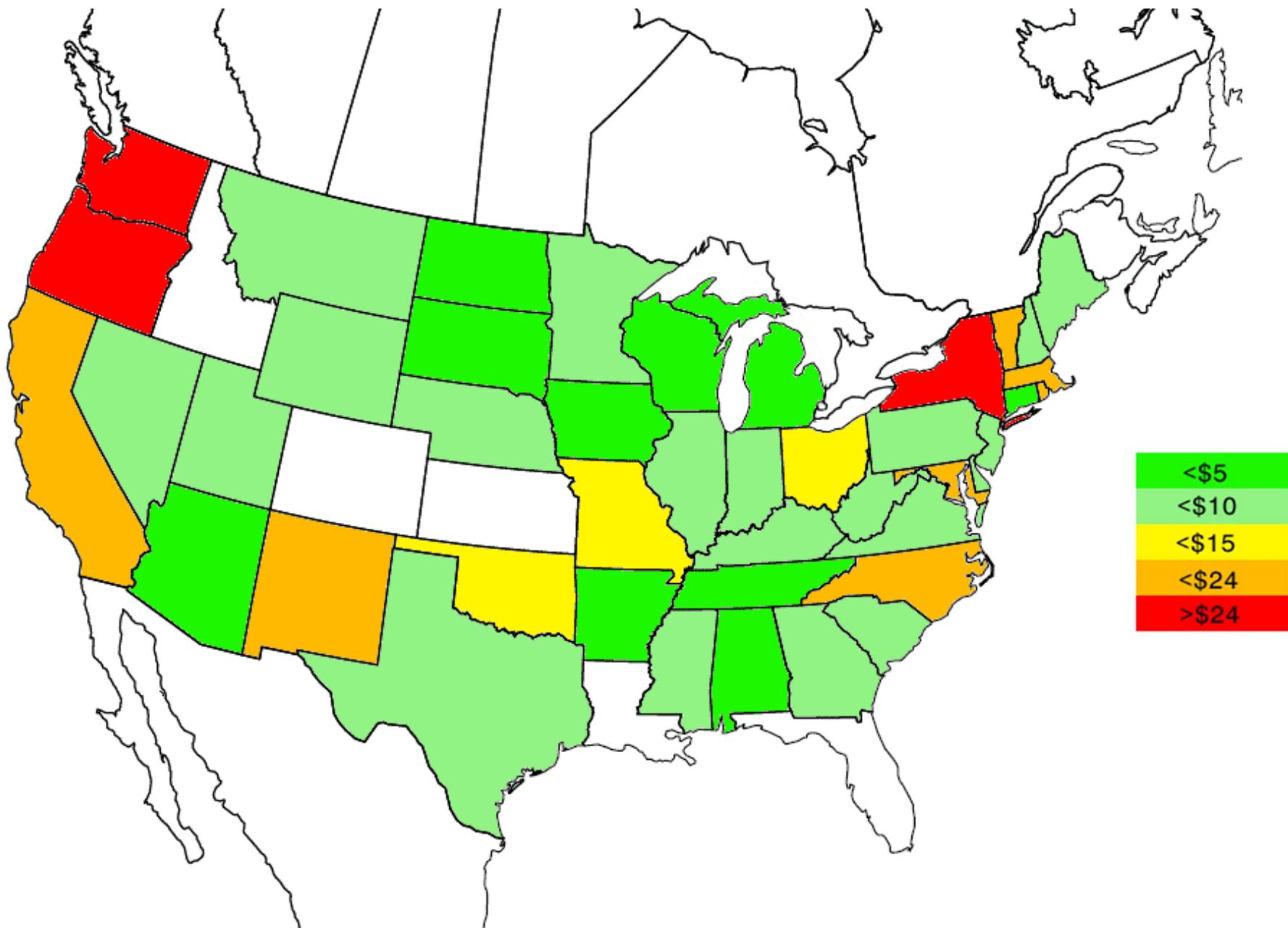
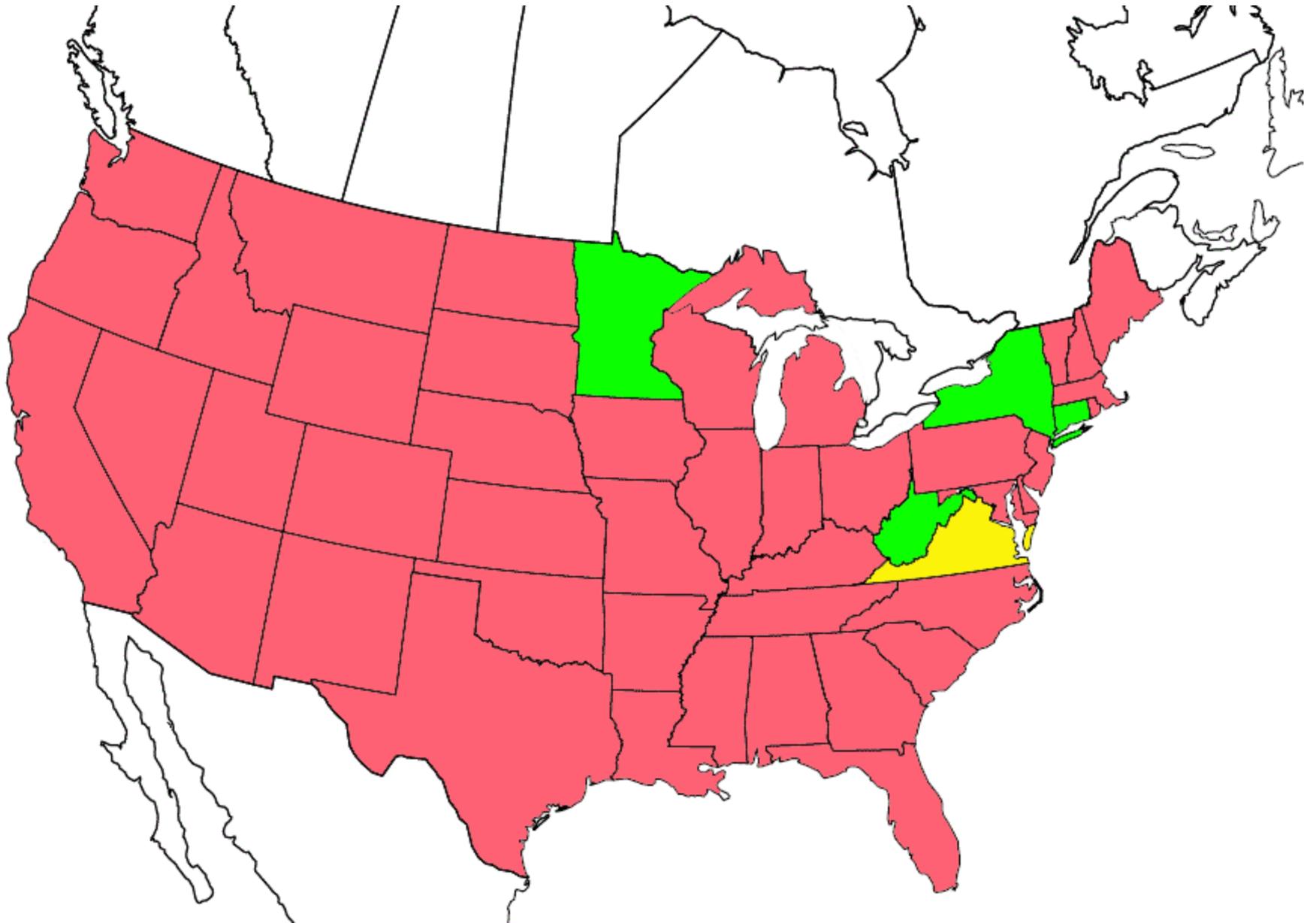


PLATE REPLACEMENT COST



**CHANGE YOUR PLATE NUMBER, CHANGE ALL
YOUR PARKING PERMITS**

8 CHARACTER PLATES

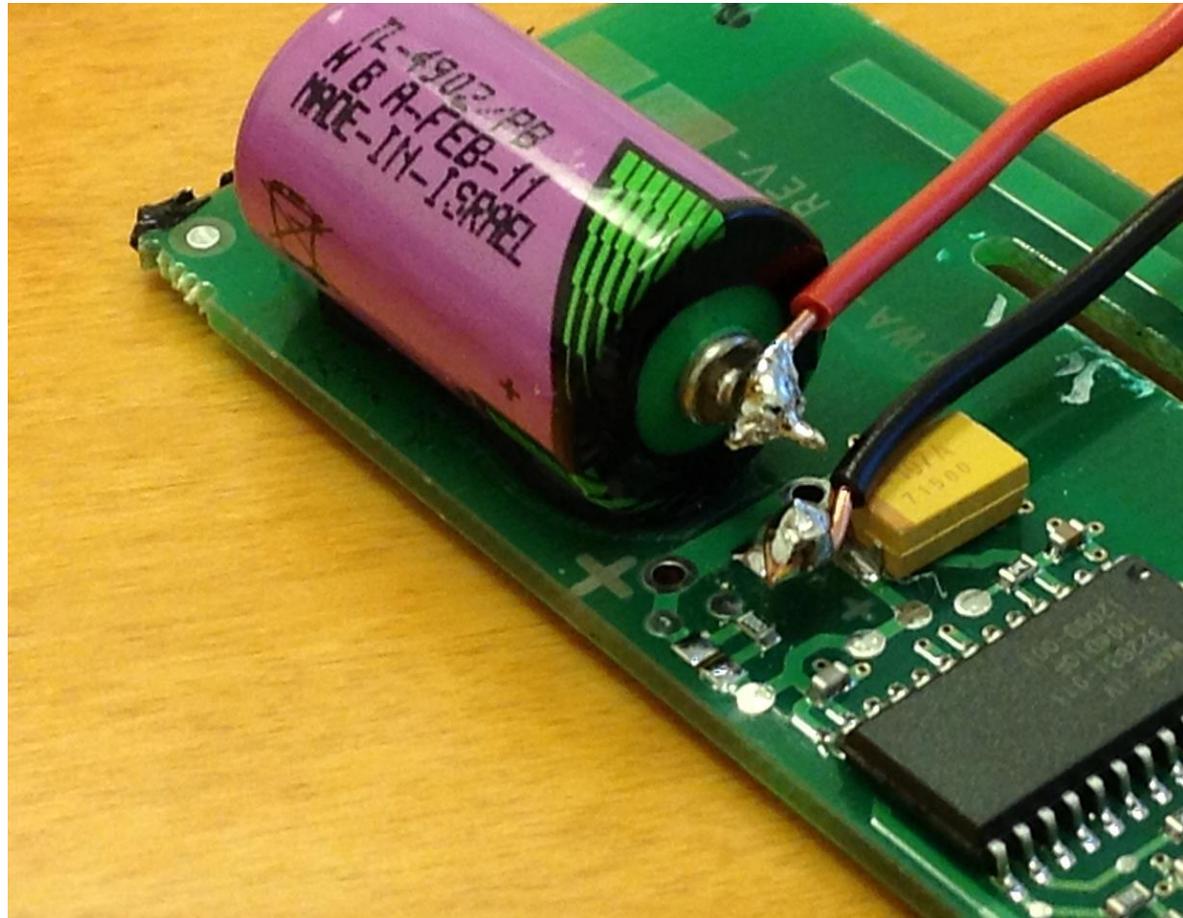


ELECTRONIC TOLL COLLECTION TAGS

- **Always on**
- **All ETC is 915Mhz in the US**
- **Multiple non-compatible protocols**
 - **Interagency Group (IAG) (E-Zpass)**
 - **California Title 21**
 - **Allegro**
 - **eGo**
- **It's RFID, some with battery assist some without**

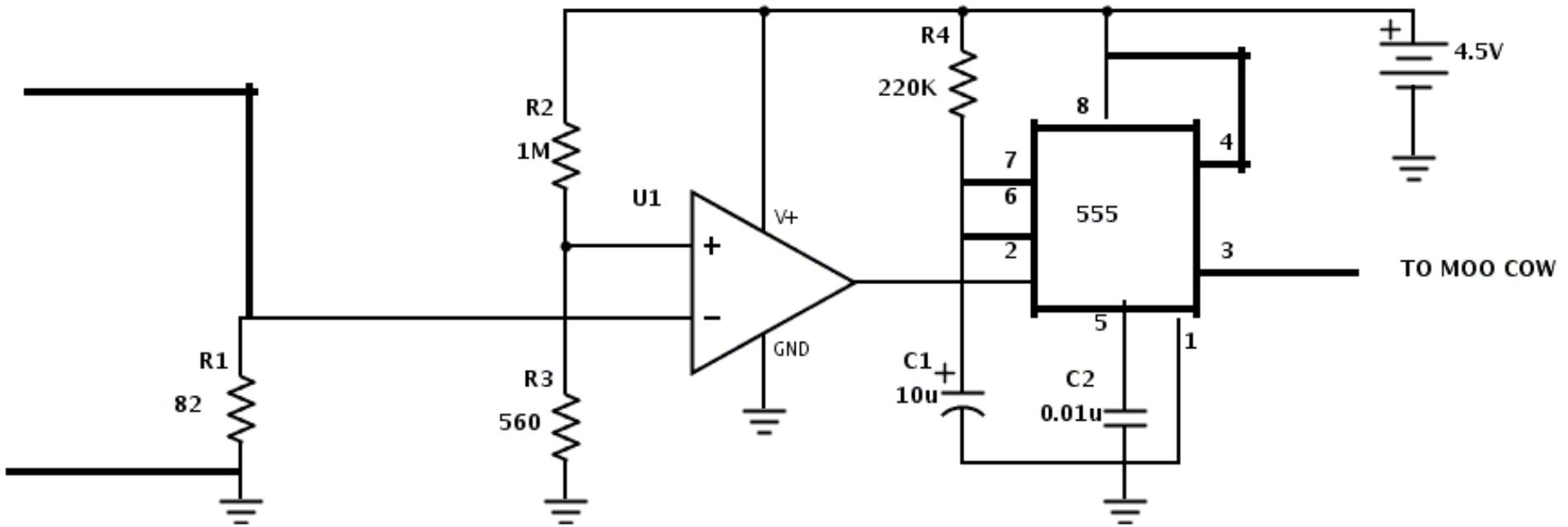
E-ZPASS TAG

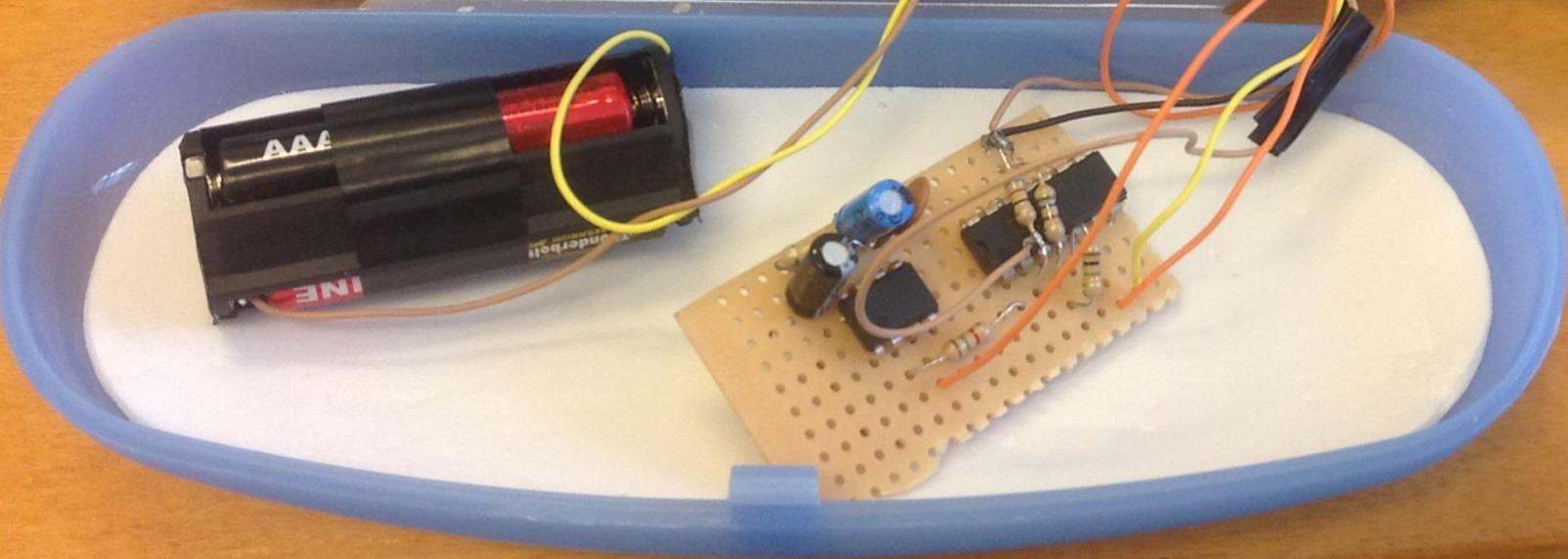
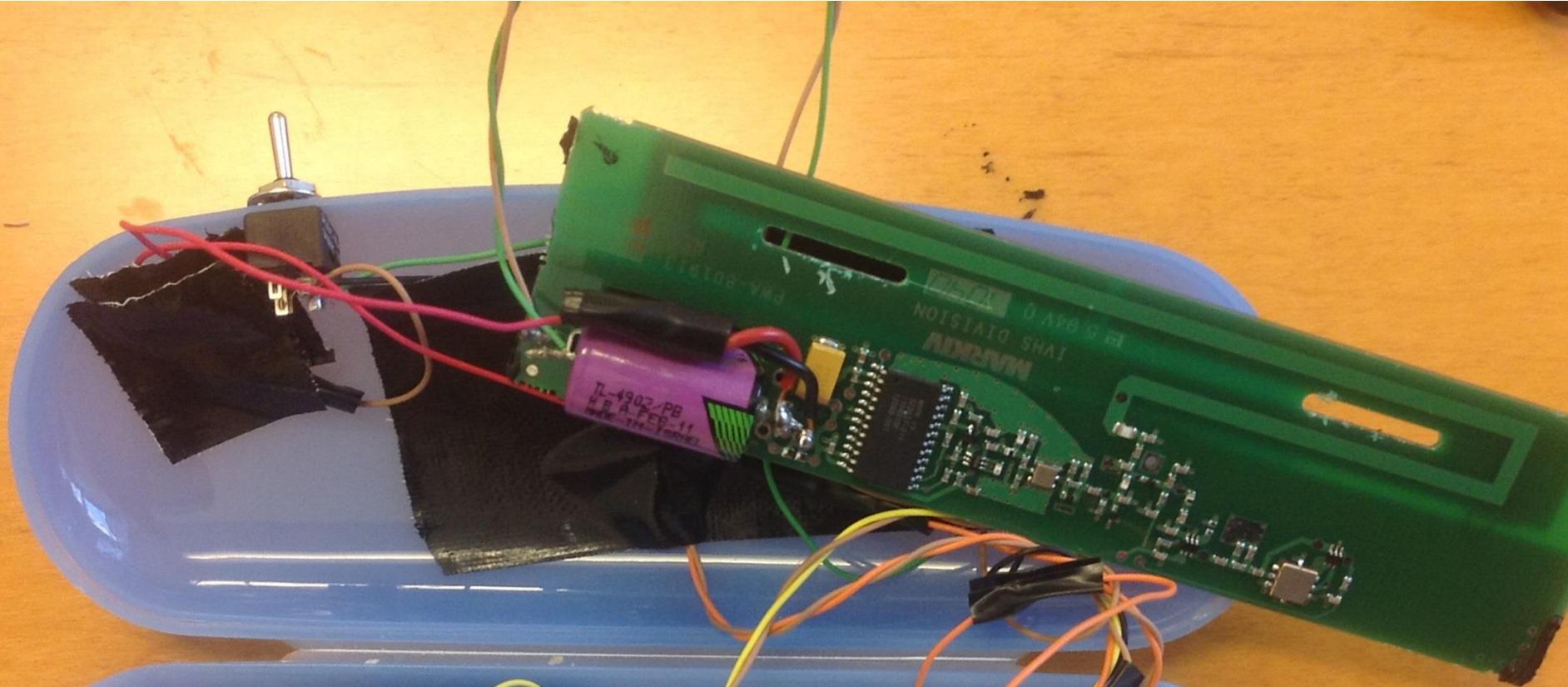
- 3.6V low draw, long life (10 year) battery
- Device draws 8 μ A quiescent
- Device draws 0.3mA when being read, transmitting
- **DO NOT DO THIS, IT IS NOT YOUR PROPERTY**



E-Z PASS READ DETECTION CIRCUIT

Low side (shunt R1 between circuit and ground)







E-ZPASS GETS READ UNDER THE SIGN, BUT NO TOLL AROUND HERE



**SO THAT'S
WHY!**



NOT SO HIDDEN, BUT NO TOLL HERE



E-ZPASS GETS READ AT 42nd & 8th

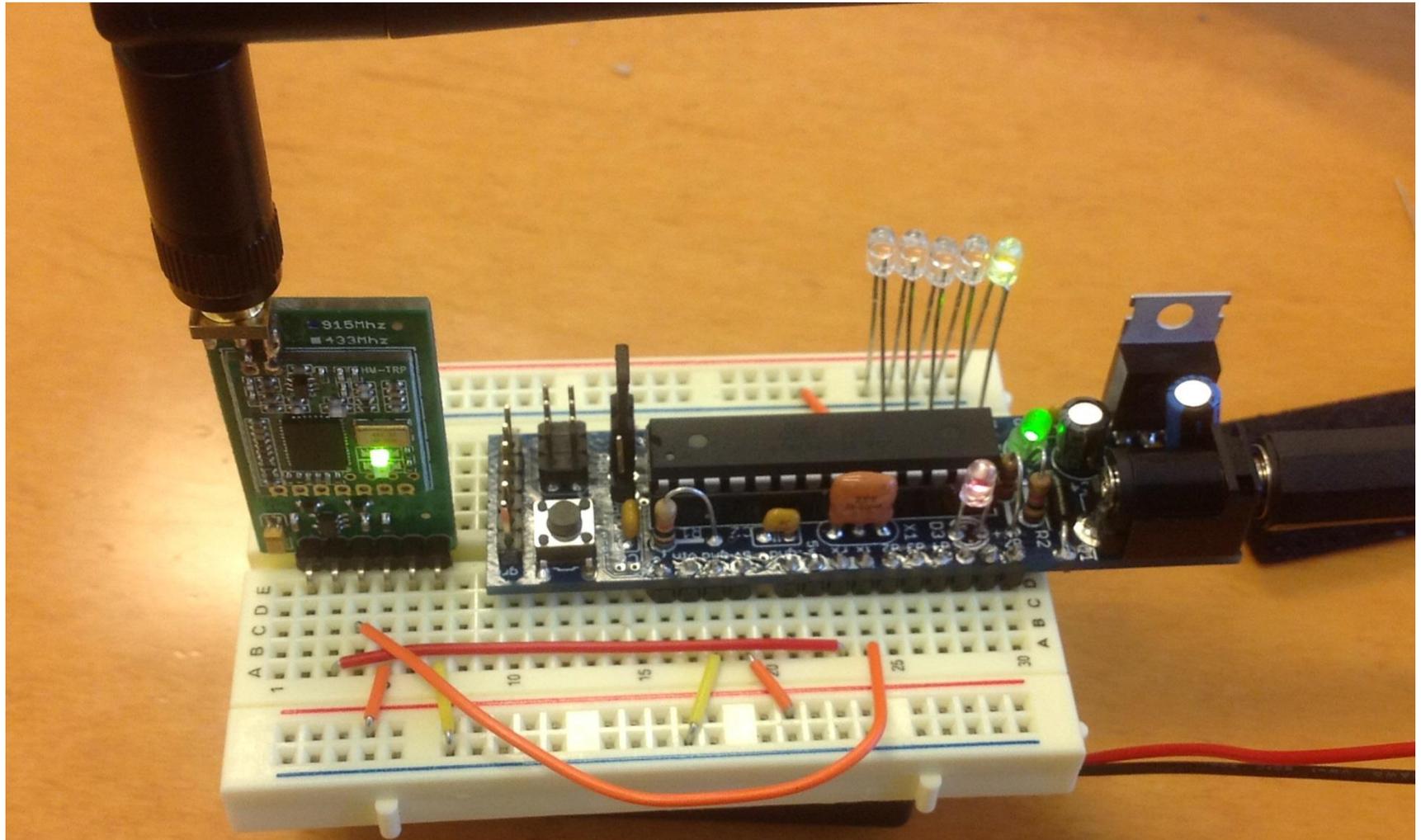


TransCore

Company can read all transportation formats, like ATA, eGo, IAG (reversed engineered), etc.



**PROBLEM WITH TAG BASED DETECTOR IS
YOU MUST BE READ TO FIND THEM
NEED A BETTER ONE**







SUGAR-FREE
ALToids
Smalls
naturally & artificially flavored
PEPPERMINT

50 MINTS
NET WT 0.37 OZ (10.5g)

42nd & 8th WITH NEW DETECTOR



- NYSDOT admits they use it for "travel time" signs
- Who else gets and what happens to this data?
- How long is it retained?



WHAT TO DO?

- Bag the tag, and only bring it out when you want to pay a toll.
- If you have a sticker build a faraday cage box that you can swing open and shut
- Remember the toll is tracking you too
- It will become obvious to “watchers” you are doing this as you will be seen at tolls but no where else

YOUR TIRES

- **Federal US TREAD (Transportation Recall Enhancement, Accountability and Documentation) law**
- **Two different things happening here**
 - **Tire Pressure Monitoring System (TPMS) 315MHz transmitter at the valve stem, not the tire, this is part of the rim. Has a battery and a unique ID**
 - **RFID in the tires themselves, unique per tire**
 - **Michelin uses 915MHz**
 - **Goodyear uses 125kHz**
 - **Auto manufactures place the VIN in these RFIDs as well**



WHAT TO DO?

- Look for RFIDs and EMP them
- Locally jam 315MHz in the wheel well



OTHER RFID

- **Parking passes, it might be an hang tag or a sticker you had to put on the glass**
- **Usually private, but found one municipally that put them in for residents to cut down on parking permit counterfeiting. It's 915Mhz too.**
- **Need to bag them too, if not in use, but a permit for public on street parking is a problem**

INRIX

- **collects position data from 100 million devices across 1.8 million miles of road**
- **Google maps uses them for traffic**
- **6 of the 8 auto companies with built-in navigations systems (like Ford, BMW and Audi)**
- **8 of the 12 top navigation apps in Apple's App Store (like MapQuest, Garmin, Microsoft and Telenav)**
- **dumb phones, without GPS and internet connections are sharing location data with them through cell towers**
- **Commercial truck fleets**

CONCLUSION

- **Salt the plate**
- **Bag the tag**
- **Zap and jam the tires**
- **Turn 'em off**