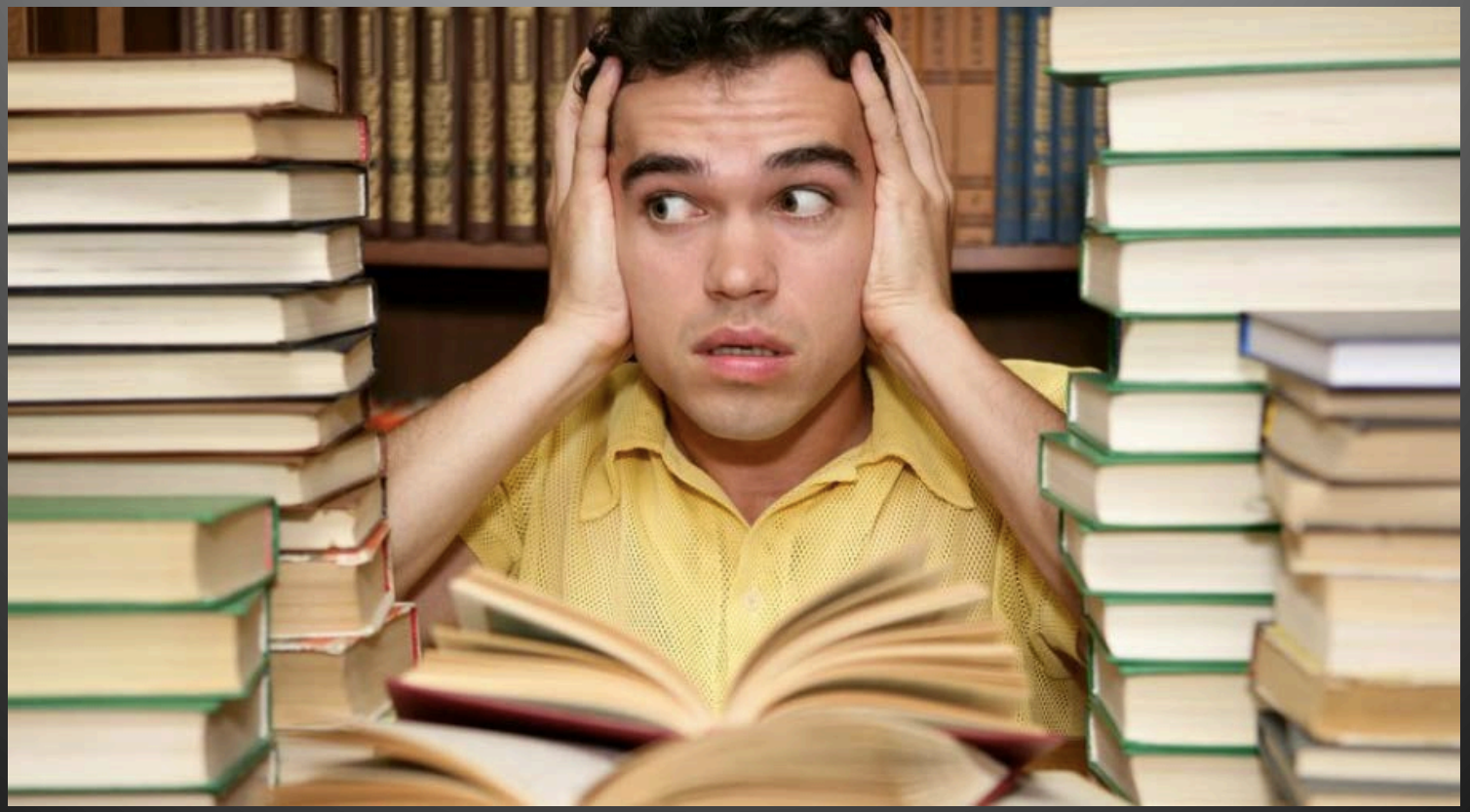
# Cross-Examination of Digital Experts

Alice L. Fontier
The Bronx Defenders

# PREPARATION OF CROSS

- NO SHORT CUT: STUDY!



# PREPARATION OF CROSS

- NO SHORT CUT: STUDY!
  - Publications on the forensic issue
  - Find and read the expert's own publications
  - Read every article cited in expert's report
  - Read the articles cited in the articles in the report

# PREPARATION OF CROSS

- Study the opposing expert
  - Bio
  - Prior testimony
  - CV
  - Publications – are they on the topic at issues
  - Bias? Always for the prosecution
  - How much money?  Is being an expert for one side the primary income

# PREPARATION OF CROSS

- Data, data, data
  - Make sure you have all of the information
  - Do not accept summary reports – get all underlying information
  - Use an expert to review the gov't information

# Cross-Examination

- I learned it all now what?

# PRELIMINARY QUESTIONS

- Can I preclude the expert
  - Is it science?
  - Is it relevant?
  - Does the proffered expert have expertise in the relevant area?
    - Pa.R.E. 702 - a properly qualified expert must possess the requisite level of “knowledge, skill, experience, training or education” to reach his conclusion.

# PRELIMINARY QUESTIONS

- How is the expert going to be used?
  - Does the evidence help or hurt?
  - Can you demonstrate that it doesn't matter
  - If it is relevant and it hurts – can you attack the accuracy of testimony?

# CROSS-EXAMINATION

- Qualifications
  - Voir dire or attack on cross
- Can the testimony help you in anyway
  - Maybe you don't need to fight
  - Focus on positives
  - Are there elements that you can work with

# CROSS-EXAMINATION

- Demonstrate adversarial bias
  - witness bias that occurs because experts are hired to persuade the claim of the hiring party in litigation; and thus, adversarial bias is presented by experts who will consciously comply their testimony with the trend of the attorney who hires them

# CROSS-EXAMINATION

- Demonstrate adversarial bias
  - Test results – are they consistently interpreted in favor of on side
  - Incomplete factual summary
  - Skewed interpretation

# CROSS-EXAMINATION

- Challenging the expert on the subject matter
  - Your expert is your best friend
  - Start with the report
  - Understand the data and claims
  - Work with expert to develop specific areas of challenge
  - Make sure the specific questions are worded artfully within the field of expertise
  - Do NOT rely solely on expert – you must be able to ad lib

# Cell Site Location Data

Strategic plan – how does this fit your theory:

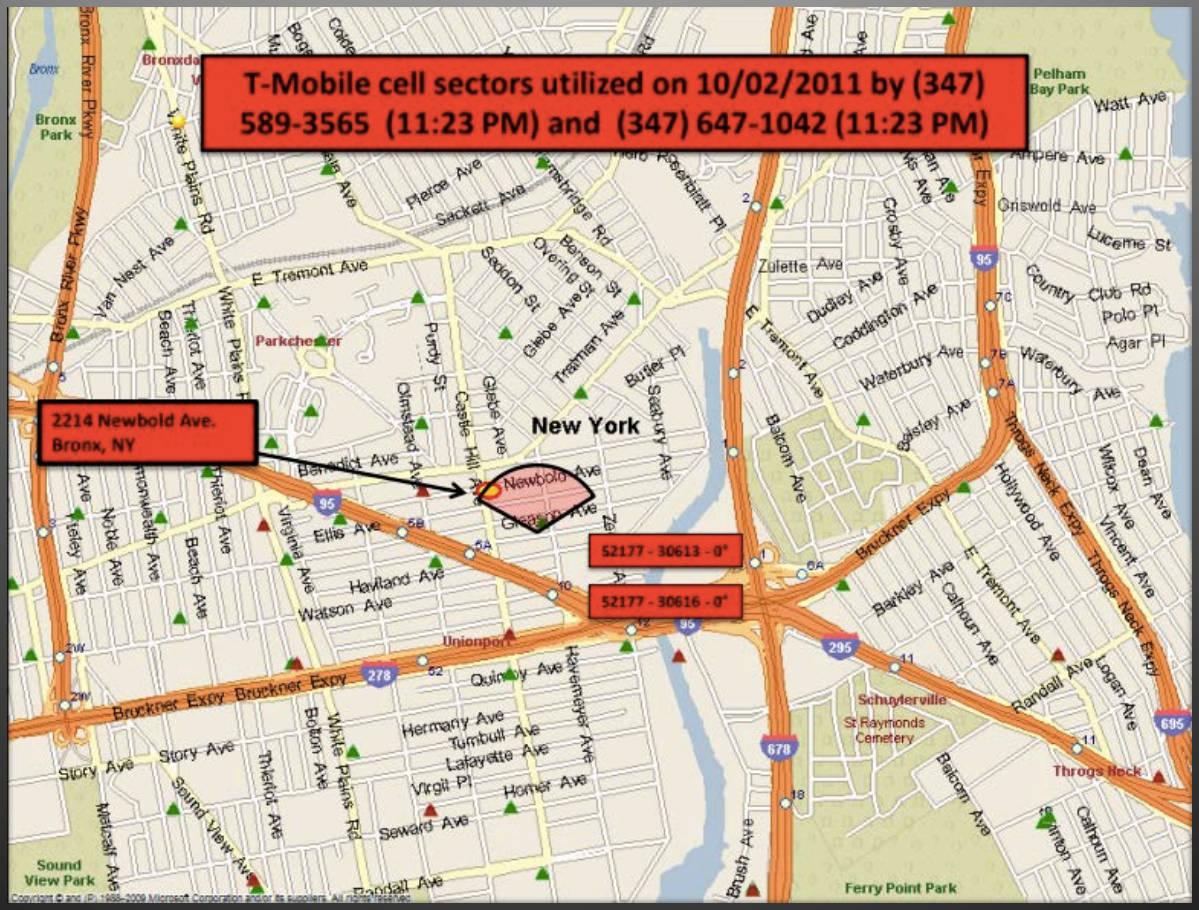
- Do you have to challenge?
  - Specific location may not be an element of the offense
  - Alternate explanation for your clients presence in the location
  - Can the location data help you?

# Cell Site Location Data

- Expand your view
  - Prosecutor will look at one point when the crime occurred
  - Look for patterns in the data
  - Is it a coincidence that client is in area

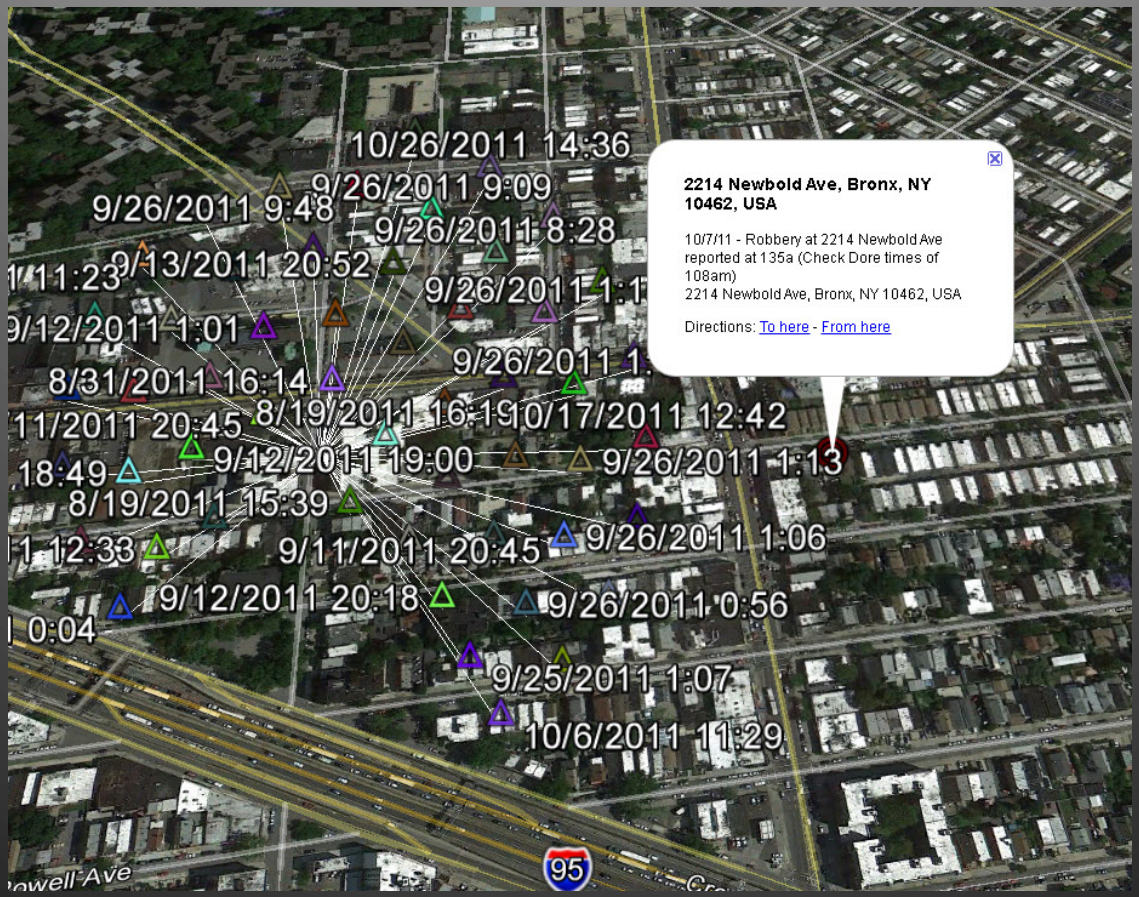
# Cell Site Location Data

Prosecution exhibit:



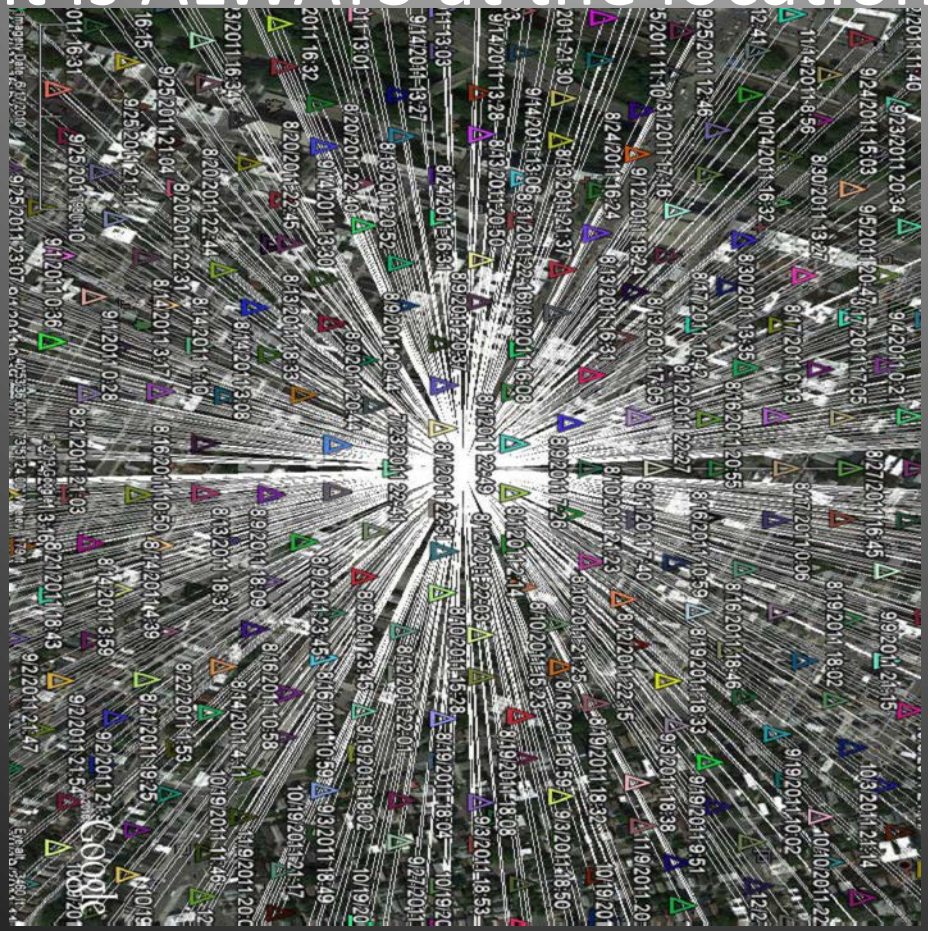
# Cell Site Location Data

- Defense exhibit:



# Cell Site Location Data

- Client is ALWAYS at the location:



Cell Tower Located at 715-719 233rd Street, Bronx, New York on 12/12/11
And Other Times
Utilized By Phone Numbers 347-883-8414 917-200-1367 and 704-345-3805

# Cell Site Location Data

- Understand the location
  - Prosecution theory is always: commission of crime is only reason to be in area
  - What else is in the area?
  - Many cell towers are attached to buildings – find out what is there and in the area around it

# Cell Site Location Data

- Location data is not specific
  - Rural and open areas have fewer towers and longer range
  - Urban areas have more interference and a greater number of towers
  - The towers are not 360 – location is directional

# Cell Site Location Data

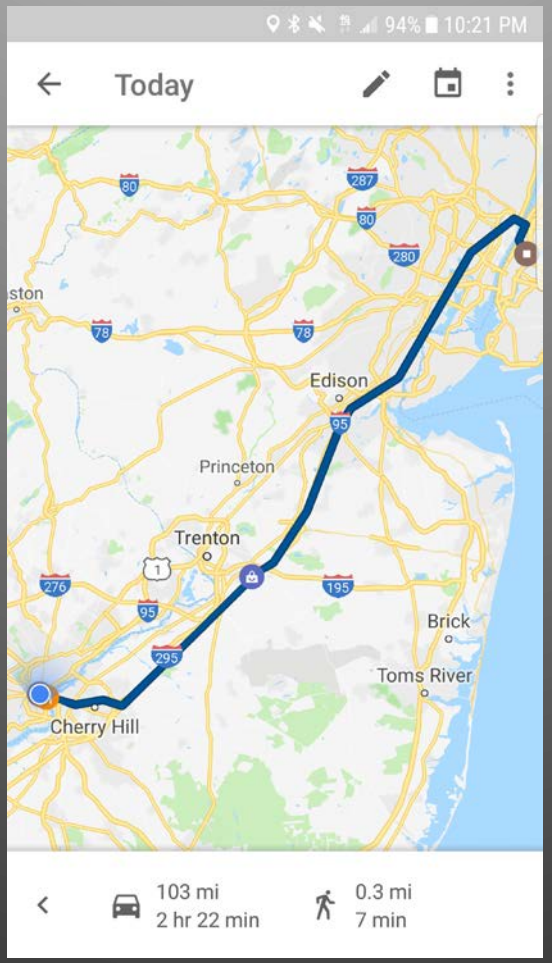
# Cell Site Location Data

- Challenging the accuracy
  - Its not science – its basic recording technology
  - But it also is not a precise location
  - Look for “jumps” in cell tower locations
    - Phone connects to strongest signal not to closest tower
    - Are there places where you can demonstrate that cell phone location could not have followed from one tower to the next

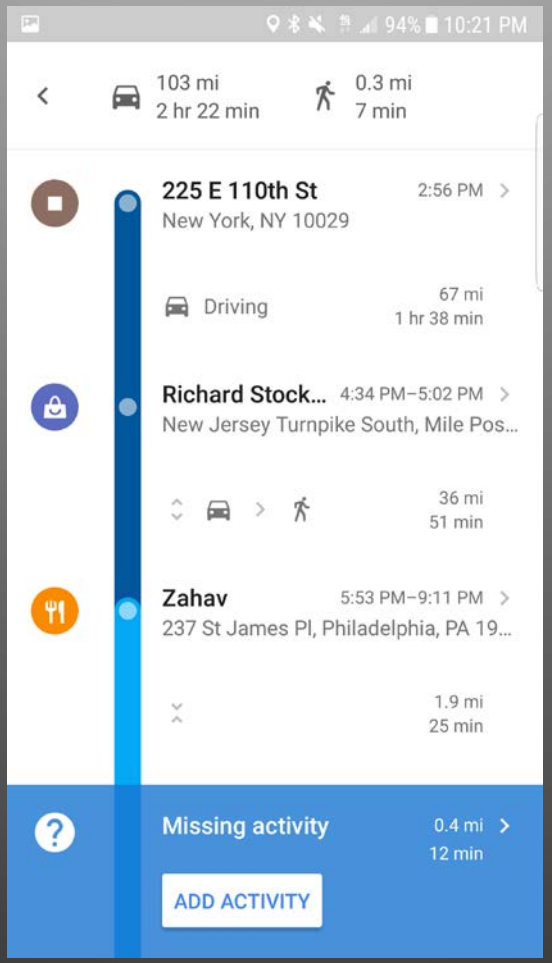
# Cell Site Location Data

- Challenge with other apps and data
  - Google map tracking
  - Standard settings create historical map of activities
  - More accurate than cell tower location

# Cell Site Location Data



# Cell Site Location Data



# Cellphone Forensics

- Cellebrite
  - Discovery:
    - CelleBrite “extraction summary report” (usually) a .pdf, .xls, or .html file). This is generated by the UFED software but can be controlled by the DT and should accompany folders containing the data described in the report.

# Cellphone Forensics

- Cellebrite
  - Discovery:
    - The investigating detectives “summary report.” This is generally a typewritten description of the request, the search performed/actions taken, and the results. It should mention the ADA requesting the search, the nature of the investigation, and the voucher numbers of the items searched.

# Cellphone Forensics

- Cellebrite
  - Discovery:
    - Handwritten “lab notes.” These are handwritten notes that should accompany the “summary report” and should describe the dates/times each action was taken and the results.
    - The “Forensic Mobile Phone Submission form.” This is the request by the DA to the DT examining the mobile device

# Cellphone Forensics

- Cellebrite
  - Discovery:
    - Grand Jury Minutes from the Investigating detective. It is usually a combination of the AO and the DT examining the device that make out the basis for the warrant.
    - The search warrant or consent/written consent to search form.
    - Photographs of the device.

# Cellphone Forensics

- Cellebrite
  - What can be extracted - live data vs hidden
  - Live data = typical user info SMS, MMS, video, email, etc
  - Hidden data = typical user cannot see e.g. web history, email headers, picture data

# Cellphone Forensics

- Cellebrite
  - Type of extraction matters
  - Logical image extraction = picture of all live data
  - File system extraction = copy of all live files and all hidden data

# Cellphone Forensics

- Cellebrite
- What was extracted and what was reported?
- The investigator can control was is extracted
  - By type - SMS, apps, MMS, emails etc.
  - By time frame
  - Review contents of report to determine what if any limitations were placed on the search

# Cellphone Forensics

- Cellebrite
  - Control by the investigator may impact your case
  - Is there missing data
  - Did client communicate over multiple mediums - e.g. SMS and MMS within one text feature

# Cellphone Forensics

## The expert - qualifications

- Expert or fact
- Ayers, Guidelines on Mobile Device Forensics, NIST Special Publication 800-101 (Revision 1May, 2014).
- CelleBrite currently has four levels of certifications in addition to miscellaneous certifications. These include:
  - beginner - The CelleBrite Mobile Forensic Fundamentals Online course (CMFF);
  - intermediate - The CelleBrite Certified Logical Operator (CCLO)
  - advanced- The CelleBrite Certified Physical Analyst (CCPA) and
  - highest level- The CelleBrite Certified Mobile Examiner(CCME).

# Computer Forensics

- Know your audience

# Computer Forensics

- What matters?
  - Typically any offense includes demonstration of knowledge or intent
- As an average computer user what do you know is on your drive?
  - Human searches - discerning them from other searches
    - URL = google/yahoo/bing

# Computer Forensics

# Computer Forensics

- Cookies
  - Stored without user knowledge
  - Explain in a way the jury can understand, e.g.:
  - searched for a pair of black boots on Zappos, the next time you sign into Facebook you see an ad for black boots … that is a cookie!

# Computer Forensics

- Look at searches in combination with cookies - is there an innocent explanation?
  - Gov't says client charged with sexual assault possessed 370 images of vaginas - how to explain?
  - Client's wife searched "symptoms vaginal pain"
  - All but 2 of the images are contained in cookies

# Computer Forensics

- Don’t forget the obvious –
  - Who has access to the computer
  - Was the image or other file sent to the person?
  - Auto save and cloud uploads? Settings and knowing control