EXAM NUMBER: _____

Problem One: SeizureSupport.com

Call of the Question

Law clerk to judge handling both cases.

Objective memo.

Bench Memo

Focus should be solely on substantive criminal law

U.S. v. Dingbat (Culpability)

Organizational Point: Three acts scrutinized.

One way to treat this is to focus on D's three potential acts to trigger 1030 liability

Act1: Initial post to SS.com message board.

Act2: Multiple infections of computers who click on link and download virus.

Act3: Logging into cruelty.net to watch webcams

Good idea to separate out, as different elements of 1030 crimes turn on the various stages, but some students might mush them all together.

Authorization

Makes sense to go access to access for this one.

Also, authorization goes to "damage" for a5A

Act1: Authorized to post to SS.com?

[Two points]

Seems to be open to the world: "on which anyone can post"

Seems not to have access restrictions or even usernames/passwords: "an anonymous user posted"

So code-based theory of authorization seems to allow this.

Might mention Morris and the "intended function" test.

Might be a norms-based theory, because you're never authorized to post a link to a virus.

Second point hard to get without making this argument.

No facts on ToS, but likely some there, so contracts/Drew discussion merited.

Act2: Authorized to install virus?

[One point]

Clearly not. Deserves very little discussion merited.

Perhaps an argument that people authorize when they click on links.

Act3: Authorized to turn on visit cruelty.net?

[Two points]

Tricky. Cruelty.net is a website run by the virus itself, so probably this part is authorized.

But Cruelty.net itself might be seen as an access to a particular victim's computer. This one it not *authorized* under any theory.

Access?

[Two points]

Might argue that Act2 (virus) isn't an access at all because the victims initiated the download

If not, then a5B and a5C for this one are not available.

Also might argue that no access of victim's computer with visit to cruelty.net, because would be streaming even if he never viewed.

Might cite some cases like Riley (used resources) or AOL (spam)

Causes the transmission?

[One point]

Paul Ohm 1/8/12 12:56 PM
Comment [1]:
2

Paul Ohm 1/8/12 12:57 PM
Comment [2]:
1

Paul Ohm 1/8/12 12:58 PM
Comment [3]:
2

Paul Ohm 1/8/12 12:59 PM
Comment [4]:
2

Paul Ohm 1/8/12 1:03 PM
Comment [5]:
1

Act2: Seems to have caused the transmission of a program, information, code, or command, satisfying actus reus of a5A.
Helps with problem of potential lack of access.

Causes damage/loss?

[Four points]

Four points only if all three points below hit.
Further: Mini-Rubric
In-depth; beautifully organized; well-written; convincing = 4
Really well done, but at least one major, conspicuous omission or flaw = 3
Hits most of the key points, but glosses over almost things too quickly = 2
Cursory or seriously incomplete = 1

For basic a5A a5B and a5C must cause damage to a protected computer
Act1: Might impair integrity of a system by posting link to virus
Proof: SS.com shut down once public learned.
But is this really the kind of "integrity" impairment Congress meant?
Act2: Seems like slam dunk. Classic type of damage.
Maybe a little nuance about fact that this virus only plays a sound file (admittedly an injurious one)
So is this really damage to computer, rather than person using computer? (this is not a winning argument, because virus did impair integrity of system)
Act3: Turning on webcam alone probably isn't separate damage above-and-beyond Act2.
But maybe some creative argument about change to privacy of computer equaling damage?
a2C requires proof of loss, which might spark some discussion of Middleton and stat. definition

A2C: obtains information from a protected computer

[Three points]

Act1 and Act2 don't seem to qualify. No information sent back.
But Act3 is focus: something is being obtained.
Slight twist that might merit brief discussion: the information doesn't reside on the computer itself. Instead, it is generated live and streamed over network.
Almost like the contemporaneous/stored distinction of Councilman.
Second point only for nuanced discussion. One for spotting at all.

Protected computer: No points, because not an issue.

Mens Rea

[Two points]

Every action here seems intentional, so second point only for nuanced theory of why mens rea might be a problem.
One possibility: no intent to shut down SS.com (if that's the damage focused on)
Another: the "access" to the virus-infected computers was not intended (Act2)

[SUBTOTAL FOR 1030 CULPABILITY]

Paul Ohm 1/8/12 1:08 PM
Comment [6]:
4

Paul Ohm 1/9/12 12:01 PM
Comment [7]:
3

Paul Ohm 1/8/12 1:12 PM
Comment [8]:
2

Paul Ohm 1/9/12 3:26 PM
Comment [9]:
17

EXAM NUMBER: _____

U.S. v. Dingbat (Sentences)

Mostly an excuse to focus on "loss" and other parts of 1030(c).

Possible sentences for (a)(5)

Base sentence for all three: one-year misdemeanor

[One point]

a5B goes to 5 years and a5A goes to 10 years if 1030c4Ai factor triggered.

Possibilities:

[Three points]

One for flagging
Two for going through some but missing many
Three for getting most of following.

III: Physical injury to any person
Not mentioned in facts, but definitely possible here.

IV: Threat to public health or safety
Good possibility found here

VI: 10 or more protected computers during any one-year
Probably here.

I: Loss of at least $5000 in value (Middleton/statute discussion)
Not clear, but worth pursuing.
Need to look at definition of loss
But not many facts to go on.

II: Modification of medical exam, treatment, or care
Possible, but a bit of a stretch.

a5A goes to 20 years if knowingly or recklessly causes serious bodily injury (c4E) or death (c4F)

[One point]

Might turn on what "sbd" means.

Possible sentences for a2C

[Two points]

Base: one year (c2A)

Up to five years if:

In furtherance of any crime or tort (c2Bii)—seems likely (iied?)
Value of info > $5k (c2Biii)—unclear from facts

Sentencing Guidelines

[Three points]

Up to three points for anything said about the guidelines.

Possibilities:

Guideline 2B1.1
Starts with base level 6
Loss chart enhancement (not clear on these facts) (CB p. 284)
+2 for intent to obtain personal information
Defined (CB286) as including "photographs of a sensitive or private nature"
If critical infrastructure, big enhancement.
But given definition (systems and assets vital to) probably not, despite "public health or safety" in definition.
CB page 287 paragraph about upward departures for "physical harm, psychological harm, or sever emotional trauma, or substantial invasion of a privacy interest."
Bottom line: less than statutory max in most cases.

Special Skills enhancement

[Two points]

Paul Ohm 1/8/12 1:19 PM
Comment [10]:
1

Paul Ohm 1/8/12 1:19 PM
Comment [11]:
3

Paul Ohm 1/8/12 1:21 PM
Comment [12]:
1

Paul Ohm 1/8/12 1:22 PM
Comment [13]:
2

Paul Ohm 1/8/12 1:23 PM
Comment [14]:
3

Paul Ohm 1/8/12 1:28 PM
Comment [15]:
2

EXAM NUMBER: _____

Dingbat doesn't seem to be all that sophisticated
Didn't cover tracks at all
Probably assisted by Unattributed
So probably not on par even with U.S. v. Lee. Nowhere near Petersen.

[SUBTOTAL FOR 1030 SENTENCING]

Paul Ohm 1/8/12 1:42 PM
Comment [16]:
12

U.S. v. Unattributed

Point of this question was to draw facts somewhere between Planned Parenthood and Carmichael, but a few other rules might also have been thrown in.
Not given the statute that gives the US Attorney the authority to do this (some students might assume this has something to do with 18 U.S.C. 875 or 47 USC 223) so focus should instead be on the First Amendment.

True Threats Doctrine

[Four points]

Is this even a threat?
Perhaps not.
Facts suggest some encouragement: "might be fun" + list of websites, plus link.
Becomes more of a threat once group ignores requests to take down.
Not nearly as overt as Red X's in Carmichael or strike-through in Planned Parenthood
Might compare Alkhabaz and 223: "serious expression of an intentional inflict bodily harm" and "effect or achieve some goal through intimidation"

Even if threat, probably not a true threat
Context is key: this is a hard-to-find website (at least until media notices it) that doesn't make a very overt threat.
Definitely not the named, killed, named, killed pattern of PP.
Not the "broad context" of Carmichael (history of violence to informants"
Reasonable person test: probably not a threat.
Mere advocacy has been held not to be enough.

Paul Ohm 1/8/12 1:39 PM
Comment [17]:
4

Incitement

[Two points]

Might be incitement instead.
Might go through Brandenburg test.
Imminent lawless action

Paul Ohm 1/8/12 1:39 PM
Comment [18]:
2

Low-Value speech

[One point]

Might analogize to obscenity or CP as low-value speech (a stretch)

Paul Ohm 1/9/12 3:26 PM
Comment [19]:
1

[SUBTOTAL FOR U.S. v. Unattributed]

Paul Ohm 1/9/12 3:27 PM
Comment [20]:
7

[Total for Problem One: SeizureSupport]

Paul Ohm 1/9/12 3:27 PM
Comment [21]:
36

EXAM NUMBER: _____

Problem Two: MyMood.com

Call of the Question

AUSA's memo to bosses assessing whether and how the FBI can make the six desired requests in compliance with:

Statutory privacy laws

The Fourth Amendment

As with Problem One, an objective memo. No need to be persuasive. But tone should be appropriate and conclusions must be drawn.

Organization

This will be tricky to grade, because there will be so much variability in the organization.

Most students will probably tackle this in order (one to six), but I think it makes more sense to tackle the big Fourth Amendment and ECPA questions about the various iterations of the service first, so that's how I'll structure the rubric.

Also useful to think of the service as having six components, labeled here with letters indicating what I'll call them from now on:

A: The fact that D owns/wears a MoodTracker

B: The raw data collected by the MoodTracker (pulse, temp, sweat, etc.)

C: The "moods" calculated by MyMood.com's algorithms (happy, sad, etc., and lying or not).

D: Personal mood store, accessible only by the user.

E: MoodTracker: Personalized website accessible only to password-authorized people of "pushed" moods (like Twitter)

F: MoodTracker-to-Email bridge

And at the end, I'll add the sections one to six, to pick up any other issues left over.

Part I: Fourth Amendment

Some of the broader Fourth Amendment issues will be scattered throughout or handled together in one place. So focus first on one big discussion to begin.

Reasonable Expectations of Privacy

REP for both the raw data and the moods calculated from that data. (B/C/D and (to lesser extent E) above)

[Six points]

Paul Ohm 1/10/12 9:41 PM
Comment [22]:
6

This was meant to be one of the big questions on the exam, so allow for lots of point collection.

Be stingy with sixth (and even fifth) points.

Only way to get all six points is to delve deeply into the policy debate around this.

Mini-Rubric

In-depth; beautifully organized; well-written; convincing = 6

Really well done, but at least one major, conspicuous omission or flaw = 5

Hits most of the key points, but glosses over almost things too quickly = 4

Misses at least one big argument, but otherwise competent = 3

Misses at least two big arguments, but otherwise competent = 2

Barely mentioned issue = 1

Subjective: Did this particular person expect privacy.

Objective: Is this expectation one that society is prepared to accept as reasonable?

Unprecedented: For data/mood, analogies to rich body of communications caselaw breaks down.

At least when we're talking only of the mood store.
Analogies to email (and esp. Twitter) work well for MoodTracker
Unlike email, which draws a direct line to postal mail, we have no history in this country of even knowing this info about ourselves, much less sharing it!
So analogies to Hoffa/Katz/Smith fall flat
How does pulse, body temp, sweat production, blood flow, and brain activity compare to the communications privacy discussed relating to email? (Like Warshak)

So what do we make of this kind of data?

Like location, this is data we rarely used to measure or track, and it's certainly nothing we've never shared. (Jones)
Strength of this varies on which piece of raw data we're talking about, and reward subtle analysis of differences (brain waves are esp. creepy)

Some of this perhaps in plain view?

None of this really seems to be plain view, despite ability by some to monitor temperature from far away
Maybe citing Kyllo's "general public use" prong here.

Raw Data versus calculated mood information (C/D not B)

Two points

I had intended for students to draw a distinction between the raw data (pulse, temperature, etc) and the calculated mood information.

But now I'm convinced that most will miss this, so two bonus points to the few who see this.

Most aggressive govt argument: no REP because not D's data at all, but instead calculations based on D's raw data.

Courts not likely to buy this, given sensitivity of information.

Might also implicate third-party doctrine (below) because raw data is apparently never revealed to anybody! Just calculated moods.

So if "consent" through any sharing, not here.

A: The fact that D owns/wears a MoodTracker

[One point.]

No REP, because in plain view. Assumption of Risk

Consent/Third-Party Doctrine

[Five points possible.]

Students are likely to mush together REP and consent, so some of this will be mushed together with six points above

Comparing this to numbers dialed (Smith) and bank records (Miller)

Nothing really seems revealed for MyMood's purposes (MyMood makes money on the initial sale, not the subsequent use)

Some discussion of Terms of Service.

Did it include any disclaimers/warnings about sharing with the police that might constitute IV consent (maybe citing Warshak's discussion)

Best answers will note how strength of this discussion varies between the three places where we find moods in this service:

D: Personal mood store, accessible only by the user.

Analogy: Seems a lot like personal file sharing sites or email in RCS-mode, so probably discuss Warshak.
Might talk about content/non-content here, and maybe even discussion of Forrester or Hambrick.

E: MoodTracker: Personalized website accessible only to password-authorized people of "pushed" moods (like Twitter)

Paul Ohm 1/10/12 9:44 PM
Comment [23]:
2

Paul Ohm 1/10/12 1:03 PM
Comment [24]:
1

Paul Ohm 1/10/12 9:59 PM
Comment [25]:
5

EXAM NUMBER: _____

A lot like email or twitter.
Password protected, restricted access should matter a lot.
Facts seem to suggest no "purely public" setting.
Does number of "followers" matter?

F: MoodTracker-to-Email bridge
Probably just a direct application of Warshak. No reason why this should be different.
Now you're translating the raw data/moods into the content of communications.
In Sixth Circuit: REP. Outside, unclear.

[SUBTOTAL FOR PART ONE/Fourth Amendment]

Paul Ohm 1/10/12 9:59 PM
Comment [26]:
14

Part II: ECPA Preliminaries

These ECPA issues will arise in different places, so have one catch-all rubric for them.

ECS or RCS?

[Four points for good analysis.]

Paul Ohm 1/10/12 1:29 PM
Comment [27]:
4

Are the various services deployed by MyMood.com ECSes, RCSes, or neither under the SCA?

D: Personal mood store, accessible only by user.
Definitely not ECS.
Probably RCS because purpose is storage and processing.
Might be an argument that isn't "solely" for these purposes.

E: MoodTracker: Personalized website a la Twitter
Much more like an ECS.
Allows only "sending" but not "receiving" of communications. Matters?
Are these communications, given limited nature?
Probably. Definition of elec. Comm.. is expansive.

F: MoodTracker-to-Email bridge:
Seems like a classic ECS.

To the public?

[One point.]

Paul Ohm 1/10/12 1:30 PM
Comment [28]:
1

Clearly to the public.
Fact that you must buy something expensive doesn't matter. Fees don't obviate public-ness.

Voluntary disclosure?

Two points

Paul Ohm 1/10/12 1:39 PM
Comment [29]:
2

Since the provider is to the public, anything stored cannot be volunteered by the provider under SCA, so process will be needed.
Only exception might be for things that aren't electronic communications at all, of which some of these might be.
But doubtful, given expansive definition.

Content versus non-content?

Two points

Paul Ohm 1/10/12 9:52 PM
Comment [30]:
2

This raw data and moods don't really fit within our classic conception of contents.
But if you really parse E.C. and E.S. closely (more closely than we did in class), you'll see the fit better.
And even if not content, probably not non-content either.

Paul Ohm 1/10/12 9:54 PM
Comment [31]:
2

Trivia about process

Two points

Up to two points for on-point, applications of rules (not just the rules) relating to ECPA process.
Possibilities (incomplete list):
D-order standards
2703(f) preservation requests
2705 delay
Civil liability and no suppression

[SUBTOTAL FOR PART TWO/ECPA Preliminaries]

Paul Ohm 1/10/12 9:59 PM
Comment [32]:
11

Part III: The six requests

(1) Temperature readings from the date and time of the bank robbery

Two points

Paul Ohm 1/10/12 1:40 PM
Comment [33]:
2

Unclear from facts: Is temp probe reading ambient (air) temperature or body temperature?
Might matter under Fourth Amendment because latter is more sensitive.
Then again, if former, don't treat this as purely public info, because it's not the temperature in a place that we're interested in, it's temperature near a person.
But then again, he's supposedly in a public place (side of a mountain) where eyewitnesses will see him and have a good guess about his temperature.
In a sense, temperature here is a stand-in for location
This is extremely subtle. One point only for those who spot this.
Not much more to say about Fourth Amendment.
ECPA
Stored, so only SCA to worry about.
Store of raw data is either RCS or neither (because not really stored on user's behalf.)
If RCS, probably "contents" and thus need warrant or subpoena/d-order with notice.
If non-content, then subpoena won't do, but no notice needed for d-order.

(2) Truth records from date/time of interview.

[Three points]

Paul Ohm 1/10/12 1:44 PM
Comment [34]:
3

Fourth Amendment
Best answers will notice the horrible atmospherics here.
We really treat lie detector tests as invasive things we limit for deeply consensual interactions (at least if Hollywood is to be believed).
Does fact that people begin voluntarily wearing lie detectors change this? Analogy to smart phones is appropriate.
Judge is likely to frown deeply on such requests.
ECPA
Stored, so only SCA to worry about.
Subtlety: Sometimes mood data is subject of ECS and sometimes RCS, depending on where in service it is.
Mood store: RCS
Mood Tracker: ECS
Assume RCS is easier here.
If RCS, probably "contents" and thus need warrant or subpoena/d-order with notice.
If non-content, then subpoena won't do, but no notice needed for d-order.

(3) Mood updates for D recorded by automated logging service

[Three points]

Paul Ohm 1/10/12 9:50 PM
Comment [35]:
3

Question doesn't restrict this just to Didit, which is what I intended to do. Don't fault students too much for failing to see this.
Fourth Amendment
Should talk about how you can't delete, and four years of information might raise new sensitivities
Citing mosaic theory/Jones
Third point only for those who spot this.
ECPA
Stored, so only SCA to worry about.
Store of raw data is either RCS or neither (because not really stored on user's behalf.)
If RCS, probably "contents" and thus need warrant or subpoena/d-order with notice.
If non-content, then subpoena won't do, but no notice needed for d-order.
Best answers will focus on justification standards
For Fourth Amendment or SCA, fact that we want his moods for all time (apparently) should make us worry about our ability to meet PC or relevance.

(4) Updates posted to Didit's MoodTracker website
[Three points]
ECPA
Stored, so only SCA to worry about.
Very likely ECS here, because point is communication.
Electronic storage
Definition: temporary, intermediate storage incidental to electronic transmission?
Seems odd to call these temporary or intermediate, given nature of service (like Twitter)
But: Theofel
Why are these stored? Any argument it is for "backup purposes"?
If yes, then everything is in electronic storage, so warrant needed.
If no, then might just be RCS uses we worry about.
If ECS in electronic storage, need warrant
If not, as below for RCS:
Might also invoke 180 day rule.
If RCS, probably "contents" and thus need warrant or subpoena/d-order with notice.
If non-content, then subpoena won't do, but no notice needed for d-order.

Paul Ohm 1/10/12 1:56 PM
Comment [36]:
3

(5) Records of average mood updates recorded for men of D's age across all of MyMood's customers.
[Three points]
Third point only for those who go well above and beyond.
Lots of opportunity for interesting discussion and policy.
Fourth Amendment
On one hand, because of effects of aggregation, hard to say that anybody has an REP in this.
On other hand, might this turn on how many men are in the population?
Some might talk about DOJ's subpoena to Google re: search terms (which we discussed only briefly).
Might also talk about lack of PC, if this is protected.
ECPA
Probably not an ECPA matter, because no "user" or "subscriber."

Paul Ohm 1/10/12 1:58 PM
Comment [37]:
3

(6) Order MyMood to increase the frequency with which MoodMonitor sends data to mood store.
[Three points]

Paul Ohm 1/10/12 1:59 PM
Comment [38]:
3

Third point only for those who go well above and beyond.
This one is really hard to analyze, so give students room for creativity.
Fourth Amendment: this is <u>much more</u> like Jones.
Causing tracking that doesn't already happen.
So even if mood store itself doesn't implicate IV, this might.
On other hand, we're not asking for the info, we're just asking that it be preserved.
Perhaps analogy to 2703(f) preservation letters.
Or maybe even analogy to debate over seizure of intangible data.
ECPA
Might be only place in exam to discuss wiretap/PT
This seems like it might be the "acquisition" of something.
But is it the contents of communications?
Remember that in the "mood store" part of the architecture, not really a communication yet, is it?

[BIG SUBTOTAL FOR PART III/Six Requests]

Paul Ohm 1/10/12 9:59 PM
Comment [39]:
17

TOTAL FOR PROBLEM TWO: MyMood.com:

Paul Ohm 1/10/12 9:59 PM
Comment [40]:
42