

EXAM NUMBER: _____

Problem One: U.S. v. David

Call of the Question

We represent David: Criminal defense attorneys

Form: Memo to Partner, so tone matters. [One point for tone.]

But because asked to assess the strength of government's case, no need to be persuasive.

Objective memo.

Focus should be solely on substantive criminal law

BUT, not perfectly clear in call, so I hope students didn't waste too much time on investigation (which wasn't really posed on facts.)

Counts One and Two: 1030

Many issues in common, so start here.

Authorization

[EIGHT points for entire discussion.]

[There are dozens of ways or organizing this, and nobody will have the room to be as exhaustive as I am in what follows.]

[SO, I will look for students who get most of what follows, and then award up to eight points on a gestalt basis.]

Rough rubric:

In-depth; beautifully organized; noticed the differences in the timeline matter; well-written; convincing = 8

Really well done, but at least one major, conspicuous omission or flaw; can't get 7 (or 8) unless they tease out distinctions between the three computers = 7

Hits most of the key authorization points, but glosses over almost things too quickly = 5

Misses at least one big authorization argument, but otherwise competent = 4

Barely mentioned authorization = 1

Both counts one and two turn on meaning of "without authorization" and "exceeds authorized access"

General Organization: Authorization may vary across two dimensions:

[Two points for noticing organization options and for executing well. But many ways to earn these two points.]

1. Which computer?

"Unrestricted"

"Restricted"

His office computer

Point about chaining: Authorization for each may be linked directly to whether he had authorization on another.

e.g., if he was authorized to access his office computer, good argument he was derivatively authorized to use Unrestricted.

2. At what point in time?

Before these events

Once he accesses Restricted for the first time

After he is fired and sent back to his office to clean his desk

Office Computer

No doubt he was fully authorized UNTIL he was fired.

After the firing, murky.

Told only to clean his desk and leave premises immediately

Told he would be thrown out as trespasser.

Comment [ohm1]:

1

Comment [PO2]:

8

EXAM NUMBER: _____

Just came in, computer was turned off, so can't argue that he was already logged in. Perhaps ask about **norms**: did he breach established norm by turning on office computer?

Maybe onus on personnel employee to tell him not to turn computer on?
Possibly citing Shurgard

Contract theory: his permission to access office computer was premised on his employment; expired when employment K expired.

Then again, when was he fired? When the personnel officer said so, or after he left the premises?

Possibly citing Shurgard

BUT, strong counter-argument available based on code restriction theory.

They could've disabled his password.

They didn't

Unrestricted computer

Before being fired

Clearly some access, just "like every employee"

"Access to his files" suggests that maybe he is supposed to keep his access only to his files.

Need more facts.

But, suggests a norms-based approach.

Employment Contract?

Government should not rely too much on this for many reasons:

1. Twelve years since signed
2. Many pages with two sentences stuck in the middle.
3. Language of term itself is vague
"please respect" is merely a request
"Access only the files you are **authorized** to access" is tautological. Not helpful.
4. Line signed says "read and understood" which isn't as clear as "I agree."

Best argument for government on K: it's labeled a contract and it mentions the network specifically.

It's called "Unrestricted" which is at least suggestive.

Password/Chaining Point:

Password is on his office computer, so in some sense, turns on all of the above analysis.

i.e., if he's authorized to use his office computer, good argument he's authorized to use Unrestricted.

After being fired

Very similar analysis to above.

Perhaps government can lose this issue on office computer BUT still win on

Unrestricted.

Sketch of theory: "Clean your desk" might extend to "virtual" desktop, but takes another step to extend to network.

Restricted Computer

Before being fired

Initial theory looks bad for our client, under any theory!

Server is called "restricted"

Norms theory: highly sensitive research materials

Citing hypothetical involving Senate staffer who accessed other party's memos:

Should've been self evident.

Even more so for the shocking nature of the specific videos in this case.

Comment [PO3]:

*

Comment [ohm4]:

*

Comment [ohm5]:

*

Comment [ohm6]:

*

EXAM NUMBER: _____

Many technical safeguards

R&D only, and David works for marketing

BUT: How much of this is known to our client?

Especially to users like David who may not even be aware of the biometrics and multiple passwords.

More facts will help: Banners? Signs on walls?

Also: The Glitch

Our arguments about glitch bestowing authorization:

A few months is a long time. Does this become implied authorization at some point?

Applies to ANY user, so it's a really bad, and you should've been required to fix. You seem negligent for not spotting this.

Does negligence like this matter?

But government's arguments in response

It's a glitch—not an intentional reconfiguration, which helps a little.

It was done by a support technician, not by a manager.

Our sur-response: But how is David supposed to know this?

Additional facts might also help

Who is this friend who passed along the info? What did he say? How did he know?

After being fired

See everything said about Unrestricted.

Also, must flesh out specifically the chained nature of this: Office->Unrestricted-

>Restricted

Mens Rea as to authorization?

[Two points.]

For both (a)(5) and (a)(2) the access must be intentional. Must the "without authorization" or "exceeds authorized access" also be intentional?

Probably. (Kerr 103) perhaps citing Sablan or Morris

If so, even if some accesses were unauthorized, did David know they were?

[SUBTOTAL FOR AUTHORIZATION (Including Tone Point)]

Rest of 1030(a)(2) Analysis (except sentencings)

[Two points for good discussion of elements]

Mens Rea

Intentionally access a computer

Seems pretty clear.

Except, perhaps not because did he know he was accessing Restricted?

Access

Shouldn't waste much time on this (some did)

Once again about chaining.

Interesting that under (a)(2)(C), the computer accessed and the computer from which information is obtained need not be the same. (a computer . . . from any protected computer)

Means: Unauthorized access for one is all they need to show, so even if court (oddly) rules that all access to Restricted and Unrestricted were authorized, but access to office computer was not, probably enough.

Obtains information?

Clearly met.

From any protected computer?

Should cite definition in (e)(2)

Clearly met here

Used in or affecting interstate or foreign commerce or communication

On a network. Enough.

Comment [ohm7]:
*

Comment [ohm8]:
*

Comment [PO9]:
2

Comment [ohm10]:
11

Comment [ohm11]:
2

Comment [ohm12]:
*

Comment [ohm13]:
*

EXAM NUMBER: _____

Maybe cite "engineering giant" to pile on.

Rest of 1030(a)(5)(B) and (a)(5)(C)

[Two points for good discussion of elements]

Mens Rea for access / authorization

(a)(5)(B)

Intentionally accesses

(a)(5)(C)

Intentionally accesses

Both seem obvious

More on Authorization: Without authorization

This does not apply to "exceeds authorized access"

This might matter, because clear David has some access:

Pre-firing, clearly to office computer and Unrestricted network

Post-firing: Unclear.

Don't award too many points for those who dwell on this, because not too much that can be said.

Good if they go through the analysis (briefly) in the casebook.

Damage?

[Three points]

Can't get all three unless noticed both arguments for damage

Cite definition from (e)(8)

any impairment to the integrity or availability of data, a program, a system, or information

First: Deleted the research folder

Pretty easy fit. Impairment to integrity and availability of data and information

BUT, mens rea for (a)(5)(B) must be reckless.

Here: Probably reckless.

Don't give too many points, because promised students that MPC mens rea niceties wouldn't figure prominently.

Second: Made access to Restricted known.

By posting the YouTube video, alerted company that this glitch exists.

So, in a sense, impairing integrity of system, data, information.

BUT, this is really about the glitch impairing these things, not really David.

Not quite as stark as in typical hacker case.

Mens Rea?

For (a)(5)(B), damage must be reckless

Research folder? Sure. Probably.

Integrity of Restricted?

Possibly.

Loss?

[Two points]

For (a)(2)(C) and for sentencing under (a)(2)(B), this is required.

No Mens rea

Definition in (e)(11)

any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service; and Hundreds of thousands of dollars of researcher time?

First, does this even fit within the category of "restoring the data"

Comment [ohm14]:

2

Comment [PO15]:

*

Comment [PO16]:

*

Comment [ohm17]:

3

Comment [ohm18]:

*

Comment [ohm19]:

*

Comment [PO20]:

*

Comment [ohm21]:

2

Comment [PO22]:

*

Comment [ohm23]:

*

EXAM NUMBER: _____

*Textually, seems like a decent fit.
BUT, maybe "restoring" means only "restoring from backup tape"
Second, does research time qualify as "reasonable cost"?
Maybe not, because they really should've backed up such valuable data.
But, courts have been pretty expansive about loss.
This isn't the kind of truly speculative, quite removed losses that courts have not counted.
Perhaps citing Nexans or Millot*

[SUBTOTAL FOR OTHER ELEMENTS OF 1030 CRIMES.]

Sentencing for (a)(2)(C)/(c)(2)(B): Felony?

Three possibilities:

[Two points]

For purposes of commercial advantage or private financial gain?

Seems unlikely on these facts

in furtherance of any criminal or tortuous act in violation of the Const or laws of the US or any state

Possibly: Section 48

But oddity here: the access came long before the intent to commit the crime.

Then again, the "obtaining" probably did further the criminal act.

Criminal Act: Possessing with intent to place in commerce.

Can't possess without obtaining.

Creative: Maybe also the tort of trespass, because he was warned he would be a trespasser.

Value of the info obtained exceeds \$5000

Unclear. Not sure what these videos are worth

BUT, the research itself was worth millions of dollars.

DO not be confused by the "hundreds of thousands of dollars" from the deleted folder.

Irrelevant to this count.

If any, five year felony.

Otherwise, can charge for misdemeanor only.

Sentencing under (c)(4)(A): Felony

[Two points]

Five factors under (c)(4)(A)(i):

Loss at least \$5000

See loss discussion above.

Very likely satisfied.

Medical

No.

Physical injury to any person

No.

Public health or safety

Doubtful. Maybe a very clever argument about protecting soldiers. Still, probably not "public health"

Used by or for an entity of the USG in furtherance of the administration of justice, national defense, or national security.

Entity of USG: Army: Check.

National Defense: Soldiers: Check.

Used by or for?

Hardest factor.

Contract with US Army

Comment [ohm24]:
*

Comment [ohm25]:
9

Comment [ohm26]:
2

Comment [ohm27]:
*

Comment [ohm28]:
*

Comment [ohm29]:
2

Comment [ohm30]:
**

EXAM NUMBER: _____

*But server is used BY a private engineering company
Maybe it is FOR*

Close call.

10 or more computers

No.

(a)(2)(C) as misdemeanor

No further problems.

[SUBTOTAL FOR SENTENCING]

[BIG SUBTOTAL FOR 1030]

Comment [ohm31]:

4

Comment [ohm32]:

24

Section 48: Depiction of Animal Cruelty

Overview

I had planned for this question to seem unfair at first until students thought about it more.

We never covered it: Unfair

BUT, it's structured a LOT like the child porn and obscenity laws we did cover.

SO, top answers should've been flexible enough to do two things:

GO through elements of a statute like we had so many times before

Analogize possible defenses (particularly under the first amendment) to the CP and obscenity cases.

Elements of Crime

[Three points.]

Creates/sells/possesses

Possesses. No problem.

OR in the text, so not a problem that creates/sells missing

Maybe a point for flagging possible complexity raised by CP/possession cases, but this one seems cut and dry

Knowingly

Yes.

Depiction of animal cruelty

Definition:

Visual or auditory depiction

Yes.

Including photo, motion picture, film, video recording, electronic image, or sound recording

Yes.

Of conduct in which a living animal

Yes.

Maybe a point for showing how it might be tricky to prove "living animal" with analogy to what has happened to cases post-FRC

Is intentionally

Probably, but also a bit tricky to prove

maimed, mutilated, tortured, wounded or killed.

Yes.

With the intention of placing that depiction in interstate or foreign commerce

Clearly met once he posts to YouTube.

Even if that might not have been his intent when he first copied. He developed that intent at some point.

Defense for religious, political, scientific, educational, journalistic, historical, or artistic value.

Comment [ohm33]:

3

Comment [ohm34]:

*

Comment [ohm35]: *

EXAM NUMBER: _____

What is Journalistic?

An extra point for those who spend a lot of time talking about YouTube and citizen journalism.

More of a stretch: educational, historical, political.

Does whistle-blowing fit within any of these three words?

Might be some room for a public policy discussion about why Congress has this requirement in the first place, as an argument in support of whistle-blowing.

Comment [ohm36]:

1

The First Amendment

[Three points]

I meant for this to be mostly about the first amendment, but it seems like students missed this. I'll give up to three points for first amendment analysis, but it might include any of the following OR a more generalized first amendment discussion

First Amendment Defense: Miller and Ferber tests

Should talk about how Miller and Ferber should come into play.

This isn't exactly Miller or Ferber, but it perhaps fit in between.

(b) seems tailored to fit the Miller test.

religious, political, scientific, educational, journalistic, historical, or artistic value

Miller itself recites:

Serious literary, artistic, political, or scientific value

Differences between Miller exception and section 48's exception:

No mention of literary!?

Odd. How important was that to the original case?

Also, because this isn't literary in this case, seems more facial than as-applied

What about things in the rest of the list that aren't in Miller: religious, educational, journalistic, historical?

We didn't discuss this, but Miller probably sets the Constitutional floor. States are probably allowed to over-protect speech as long as they don't tread on some other Constitutional value.

Should at some point note that this can be both a facial and an as-applied challenge.

Community Standards?

Fine that there isn't talk of community standards, because policy seems different.

Absolute bar on depictions of animal cruelty doesn't seem to raise same concerns as depictions of sex. In other words, hard to imagine too much variation between types of depictions.

Hunters?

Ferber is different.

Policy is about protecting the abused.

Seems much closer to this one. But are animals the same as kids?

Mere Possession?

Rules:

Stanley: Can't prohibit mere possession of obscenity.

CP: Can prohibit mere possession of Child Porn.

Again, this is probably closer to Ferber than Miller.

KEY POINT: And this isn't just mere possession. It's possession with intent to distribute.

More like 2252(a)(3) than (a)(4)

First Amendment Defense: Free Speech Coalition/Virtual CP

Potentially a problem, because "depiction of animal cruelty" might be broad enough to encompass purely virtual depictions.

Definition probably cures this by invoking a "living animal"

Comment [PO37]:

3

Comment [ohm38]:

*

Comment [ohm39]:

*

Comment [ohm40]:

*

EXAM NUMBER: _____

But, oddly, the phrase "conduct in which a living animal" isn't completely cut and dry. Then again, it's almost definitely covered.

Policy

Ferber was "intrinsically related" to the sexual abuse of children

FSC didn't find the same intrinsic relationship.

Maybe a little about the Court's treatment of the "prosecutorial difficulties" arguments in FSC (and in particular, Thomas's concurrence).

Again, point for nuanced discussion of distinction between as-applied and facial challenges (both present here)

[BIG SUBTOTAL FOR SECTION 48.]

TOTAL FOR PROBLEM ONE: U.S. v. David:

Comment [ohm41]:

7

Comment [ohm42]:

31

EXAM NUMBER: _____

Problem Two: #entourage warez

Call of the Question

AUSA's memo to bosses assessing whether the investigation violated any:

Statutory privacy laws

The Fourth Amendment

Remedies to Defendants should also be discussed

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

[One point for proper tone.]

Organization

Two defendants

At least five different actors

Ari

Agent Vincent

Billy Walsh (runs hosted-chat.com)

MillerGold ISP

Agent Lloyd Lee (Finland)

At least six different investigative steps

For each step, Fourth Amendment, Wiretap, Pen Register, SCA

Can organize it along any of these three, but I think Act by Act makes the most sense.

Part I: Real-Time Surveillance

Just a scoring convention. Clump first three acts just for calculating a subtotal.

Act Zero: Ari's Tips

Fourth Amendment

[One point.]

Tips are not a problem because there is not argument that this is government action.

No prior knowledge or acquiescence

Act One: Vincent monitors the chat room.

Fourth Amendment

[Four points for good analysis.]

REP in a chat room?

Maybe some discussion of subjective/objective expectations

Subjective:

Lots of people coming / going; then again, passwords

Objective:

Society probably wants us to be able to have analogs of private places to chat online?

Could easily go other way.

Usually, not, assumption of risk (AoR) and *Hoffa*

But first wrinkle: password-protected

How many people have the password? How hard is it to get?

Best answers will supply analogies: after being given a key, can you open a warehouse?

(Katz and phone booths?)

Ari's mystery identity factors into this.

Second wrinkle: stealth-mode

Cuts either way...

Cuts against AoR if they can't see that a stranger has entered the room.

Then again, maybe cuts in favor of AoR? Stealth mode is known, so maybe people shouldn't just depend on the list of participants?

Comment [ohm43]:

1

Comment [ohm44]:

1

Comment [ohm45]:

4

EXAM NUMBER: _____

Maybe they should assume it's like a public space / 21st Century version of a park?

Wiretap Act / Pen Register

[Two points]

Prima facie?

Prospective, real-time, acquisition of contents.

Defenses/Exceptions?

Consent of party to communication?

Vincent's probably not a party—invisible and not talking.

Ari's not a party, because he's not listed.

Readily accessible to the general public?

We didn't really talk about this, so don't credit it too much.

Probably a violation

Act Two: Billy's month-long surveillance of chat room

Fourth Amendment

[One point]

Private search

Before first contact with FBI, so no Jarrett problem.

Wiretap Act / Pen Register

[Four points]

Prima facie?

Prospective, real-time, acquisition of contents

Defenses / Exceptions?

Provider / Protection of Rights and Property

"Because he doesn't tolerate criminal behavior on his site"

Is this a Right? A Property interest?

Possibly doesn't want to be liable for acts of others? Doesn't want to be shut down or shunned.

Provider/Rendition of service?

Doesn't seem like it.

Consent of party?

Clearly not. Administrator privileges.

He doesn't even know the password.

Same analysis about Ari as in above.

Consent through ToS?

No ToS.

Might mention this in another section.

SCA

[Two points.]

Is this voluntary or compelled disclosure?

Hosted-chat is to the public / public provider

So Billy can't disclose contents in electronic storage or non-contents of users without falling into one of 2702's exceptions.

Good argument that these were in electronic storage.

Rights and property exception also in 2702, so similar discussion to that in Wiretap.

Possible violation.

Act Three: Pen Register and Trap and Trace Order for hosted-chat.com

Procedure for obtaining order

[One point]

Certifies relevance, which is what statute requires.

Comment [ohm46]:

2

Comment [ohm47]:

1

Comment [ohm48]:

4

Comment [ohm49]:

2

Comment [ohm50]:

1

EXAM NUMBER: _____

Evidence so far is a little thin, but it's probably relevant.

Sixty days is fine. 3123(c)

Scope of order / DRAS

[Three points]

Test: Dialing / Routing / Addressing / Signaling and not including contents?

Facts are a little unclear. Students get full credit either way they read it:

This is a separate logfile that tracks transfers only, which makes this all seem pretty DRAS-like.

OR, this is a sniffer watching the chat room itself, noting files transferred. In that case, doesn't seem very DRAS-like.

User requesting contents?

Probably not. Doesn't fit DRAS.

*Also, by knowing they requested contents, probably had to look at context/contents
-> Wiretap.*

User sending file?

Same

Name of file transferred?

Even easier. NOT DRAS

Size of file transferred?

Perhaps. Closest to "signaling" but probably not.

Because of ambiguity, just give them full three points if they engaged this deeply.

Fourth Amendment?

[Two points]

This probably falls outside Smith and Miller

Nothing is being "disclosed" to third-party for third party's use.

So likely violation?

No credit for subpoena discussion, because we didn't do it in class.

Likely conclusion:

Illegal wiretap.

[BIG SUBTOTAL FOR PART ONE/Real-Time (including tone)]

Part II: Stored and Foreign Surveillance

Act Four: Grand Jury Subpoena to hosted-chat.com

SCA

[Three points]

Basic subscriber info is discussed three times, in Acts 4, 5, and 6.

You need to march through this in detail once and flag it the other two times to get all three points.

A point deducted if you forget to do this once, even if only by reference.

Is hosted-chat.com an ECS?

Clearly. Send/receive electronic communications.

Chat messages

Files

Is hosted-chat.com an RCS?

Probably not. What storage? What processing?

GJ Subpoena standard met?

Yes. Mere relevance. Easy.

Can obtain IP addresses with subpoena?

Sure. See SCA chart.

Basic subscriber information. 2703(c)(2)

Comment [ohm51]:

3

Comment [ohm52]:

2

Comment [ohm53]:

21

Comment [ohm54]:

3

EXAM NUMBER: _____

"temporarily assigned network address"

Fourth Amendment

[One point]

*Not protected. IP addresses are Smith/Miller
Might do this under Acts Five or Six*

Comment [ohm55]:
1

Act Five: Subpoena to MillerGold

SCA

[Points doled out above.]

Is MillerGold an ECS?

Presumably

Is MillerGold an RCS?

Yes. E-mail provider for Eric Murphy.

GJ Subpoena standard met?

Yes. Mere relevance. Easy.

Obtain name of user with subpoena?

Sure. See SCA chart.

Basic subscriber information. 2703(c)(2)

"name"

Comment [ohm56]:
*

Act Six: D-Order to MillerGold

SCA

D-order standard met?

[One point.]

Might spend a little time summarizing what we know up to now.

Some holes in suspicion

Vincent sees nobody transferring files

Billy tracks names of suspicious files

Pen Register turns up big files.

But this probably meets D-order's standard

Obtain all basic subscriber information with d-order?

[Points doled out above.]

Sure. SCA chart.

"any means available under paragraph (1)

Copies of all emails stored in hosted email account.

[Three points]

Must talk about Theofel

Go through general reasoning and describe differing approaches.

MillerGold is in the Ninth Circuit, but magistrate judge is in NY

If Ninth Circuit rules upheld, then d-order shouldn't ever be used for stored e-mail unless > 180 days old.

Even if pre-Theofel rules, still probably a violation because "copies of all e-mail messages"

Unread email messages shouldn't have been produced.

Bottom-line: Some violation likely.

Comment [ohm57]:
1

Comment [ohm58]:
*

Comment [ohm59]:
3

Fourth Amendment

Is the email inbox protected by REP?

[One point for flagging]

Act Seven: Surveillance/Search in Finland

Fourth Amendment

[Two points]

Comment [ohm60]:
1

Comment [ohm61]:
2

EXAM NUMBER: _____

One point for flagging, even if they forget Verdugo.

Verdugo-Urquidez: Fourth Amendment doesn't apply to non-citizens.

Turtle is a Finnish citizen

If only mention this, one point.

Two possible wrinkles to pick up additional point (don't need both wrinkles):

At time Vincent called Lloyd, he didn't know the target was a non-citizen. He only knew he/she was using a Finnish IP address.

Lloyd used an American-based chatroom service, but clearly not enough!

So confusing test of Barona not needed.

Wiretap or Pen Register?

One point.

Seems like a wiretap or Pen Register

But probably no extraterritorial application

[BIG SUBTOTAL FOR PART II/STORED and FOREIGN]

Comment [ohm62]:

1

Comment [ohm63]:

12

Part III: Remedies for Potential Violations

So lots of potential violations:

Fourth Amendment

Act I: Chat Room

Act III: Invalid Pen Register

Act VI: Email messages in Eric's account.

Wiretap Act

Act I: Chat Room

Act II: Billy's surveillance

Act III: Invalid Pen Register

Pen Register Act

Act III: Invalid Pen Register

SCA

Act VI: Copies of all email messages stored in Eric's account

Remedies

For Fourth Amendment violations

One point

Not really much focus in this class.

Suppression

Civil suit

Fruit of the poisonous tree

For Wiretap Act violations by Vincent

Two points

No Suppression for Electronic (2515)

Possible (unlikely) criminal punishment

Possible civil suit

For Wiretap Act violations by Billy

One bonus point to anybody who spots this.

Separate violation for disclosure

Giving this to Vincent might be separate violation of 2511(1)(c) and (1)(d).

For Pen Register Act violations

One point

No Suppression

Possible (unlikely) criminal punishment

For SCA violations

Comment [ohm64]:

1

Comment [ohm65]:

2

Comment [ohm66]:

1

Comment [ohm67]:

1

EXAM NUMBER: _____

[One point]
No Suppression
Possible civil suit

[BIG SUBTOTAL FOR PART II/STORED and FOREIGN]

TOTAL FOR PROBLEM TWO: #entourage warez:

Comment [ohm68]:
1

Comment [ohm69]:
6

Comment [ohm70]:
39