Ethics, Law, and Policy in Cyberspace
Final Exam

Abraham J. Reines

July 28, 2024

Part A

Question 1

Was the judge correct in finding that an enforceable contract existed between Megacorp and Mesoco? Between Nanotechnocrats and Microdev?

The elements of a contract - offer, acceptance, consideration, and mutual intent - must be examined thoroughly to determine if an enforceable contract existed:

Megacorp and Mesoco: Jim (Mesoco) communicated to John (Megacorp) for a proposal in middleware development contract. Megacorp accepted Mesoco's offer January 16th, by agreeing to terms. The contract detailed $9,243,678 and an incentive fee of $1,663,860. Both parties negotiated agreements and accepted terms; mutual intent existed at the time of acceptance.

- **Offer:**
  - January 8, 2021: Jim (Mesoco) communicated with Bill (Microdev), informing a proposal for middleware development as part of contract between Mesoco and Megacorp.
  - January 10, 2021: Microdev quoted Mesoco $1,627,288 for middleware development.
  - January 13, 2021: Barbara (Nanotechnocrats) offered to do database integration work for $123,000.
- **Acceptance:**
  - January 16, 2021: Megacorp accepted Mesoco's offer by agreeing to terms.
  - January 17, 2021: Mesoco accepted Microdev's offer.
  - January 17, 2021: Microdev accepted Barbara's offer.
- **Consideration:**

- January 16, 2021: contract detailed $9,243,678 for project with an incentive fee of $1,663,860. This amount represents consideration for services to be performed.

- **Mutual Intent:**
  - January 16, 2021: The negotiation/agreement on terms between Megacorp and Mesoco represents mutual intent to enter into a contract.
  - January 17, 2021: The acceptance of offers and agreement to terms between Mesoco and Microdev, and between Microdev and Barbara, indicate mutual intent to enter into contracts.

Conclusion: The judge was **correct** in finding an enforceable contract between Megacorp and Mesoco.

Nanotechnocrats and Microdev: Barbara (Nanotechnocrats) offered database integration for $123,000. Microdev (Bill) accepted Barbaras offer on January 17th. The agreed payment was $123,000 for integration. Email exchanges between Kathy and Barbara with acceptance of contract confirms mutual intent.

- **Offer:**
  - January 8, 2021: Jim communicated with Bill on a proposal for middleware development contract for Megacorp.
  - January 13, 2021: Barbara offered to do database integration for $123,000.

- **Acceptance:**
  - January 17, 2021: Microdev accepted Barbara's offer for database integration work.

- **Consideration:**
  - January 17, 2021: The agreed payment of $123,000 for database integration work represents consideration.

- **Mutual Intent:**
  - January 17, 2021: The acceptance of Barbara's offer and agreement on terms between Barbara and Microdev indicate mutual intent to enter into a contract.

Conclusion: The judge was **correct** in enforcing contract between Nanotechnocrats and Microdev.

Question 2

Was Trial Judge correct in ruling that Megacorp owed Mesoco $10,317,873?

Megacorp agreed to pay $9,243,678 maybe with incentives. Unfortunately, project was delivered late, and only eight of ten performance metrics were met.

The contract specified partial payment of incentive fees based on performance/timeliness. Mesoco's costs plus eight tenths of performance incentive fee and reducing cost incentive fee were calculated.

$$\begin{aligned}
\text{Base Cost} &= \$9,243,678 \\
\text{Total Incentive Fee} &= \$1,663,860 \\
\text{Performance Metrics Met} &= 8 \\
\text{Total Performance Metrics} &= 10 \\
\text{Performance Incentive} &= \left(\frac{8}{10}\right) \times \left(\frac{1,663,860}{4}\right) = \$332,772 \\
\text{Total Owed} &= \$9,243,678 + \$332,772 = \$9,576,450
\end{aligned}$$

Conclusion: The judge's calculation was based on contract terms; ruling **correct** in principle.

Part B

Question 3

Billy sues Harry for copyright infringement. What is Billy's best legal argument?

Billy owns copyright to materials on Selfies R Us. Harry copied a selfie from Selfies R Us without permission. Harry reposted and used selfie in his analysis.

Best Argument: Billies best legal argument is Harry's use was unauthorized, infringing on his copyright by republishing copied/protected material without permission. This unauthorized use violates Billy's rights as the copyright holder. Billy's rights to control use of his copyrighted material and reputation from false/damaging statements have been infringed upon by Harry's actions.

Question 4

In his defense at trial, Harry claims that his downloading and subsequent use of selfie was a fair use of picture. What result and why?

To determine whether Harry's use of the selfie constitutes fair use, we must consider the four factors of fair use as outlined in 17 U.S.C. § 107.

Harry using the picture for criticism/commentary is transformative. Although Harry has a commercial website; the transformative nature and use of the picture is considered fair use. Harry used entire work, which is not considered fair use. This being stated, the entire image may be necessary for Harry to provide an effective commentary. Harry's use did not

significantly affect market value of selfie. The use was for criticism, which is not a substitute for the original work.

Conclusion: Considering the four factors, Harry's use may be fair use because it was transformative, served a critical, public-interest function without harming the market for the original selfie.. However, the fact he used the entire work is not fair use. It's essential to remember the application of fair use is not always straightforward, depending on specifics of each case and the opinions of the court! Therefore - keeping in mind, realistically, the court's opinion may be swayed either way - given the transformative purpose and minimal impact on the market, it is more likely the court would find Harry's use to be fair use.

Question 5

Harry sues Billy for defamation. What result and why?

Billy besmirched Harry's character by denigrating his mental stability. Billy published these statements on his website. Harry's reputation was harmed by the statements. Billy made claims about Harry, stating Harry is a fraud, a possible foreign agent for Russia or China, and he suffers from a disgusting venereal disease. In a defamation claim, these statements are proven false.

Conclusion: Billy's statements are defamatory as they were false, published, and damaging to Harry's reputation. These facts align with the elements of defamation.

Part C

Question 6

Should unwitting participants of online malicious activities be held negligently liable?

Let's conduct an analysis here: Individuals have a duty to avoid negligent actions which cause harm. Clicking on malicious attachments breaches this duty. The breach directly initializes propagation of attacks. Significant harm results from these actions.

Participants in online malicious activities are negligently liable if:

- They had a duty to exercise caution.
- They breached this duty by acting carelessly (e.g., clicking on a malicious attachment).
- Their actions directly caused a cyber-attack.
- The cyberattack and resulting damages were measurable.

Conclusion: Unwitting participants **should** be held liable to negligence!

Question 7

Should companies with large IT systems be held to same duty of care as individuals with a single device?

Let's conduct a thorough analysis: Companies should have a higher standard; these companies are impactful and have greater resources available. Larger systems can cause greater harm; this necessitates stringent controls. Larger companies, managing complex IT and sensitive data, have substantial resources, face stringent regulations, and must implement security measures due to their significant impact, while individuals handle limited data and resources, follow simplified cybersecurity practices, and face fewer requirements and lower accountability.

Conclusion: Companies **should** be held to a higher duty of care.

Question 8

To what extent should ISPs be held liable under an updated Communications Decency Act of 1996?

Analyzing: The Communications Decency Act (CDA) of 1996, specifically Section 230, provides immunity for online service providers from liability for user-generated content, fostering innovation and also detailing the threat and spread of harmful content and adequacy of content moderation. ISPs should take security practices seriously. They must conduct regular security audits, and respond promptly to security incidents. ISPs should educate users about cybersecurity threats.

However, liability should be balanced. While ISPs must have security measures, users bear responsibility for their actions online.

Conclusion: ISPs should have limited liability, enforcing strong security practices. ISPs need freedom to develop new technologies without excessive legal penalization so innovation may flourish!

Part D

Question 9

Discuss ethical considerations associated with policy development for ID/Authentication.

Here are some points for an ethical discussion: Makes sure there is maximum security and benefits for the majority. Duty to protect user data and proper authentication methods. Promotes trust and integrity in system access. Social contracts require secure ID/authentication. Focuses on protecting vulnerable users. The development of an ID/Authentication policy needs security benefits to minimize harm of users, uphold the duty to protect user data through reliable processes with compliance in legal standards, foster integrity by promoting transparency in authentication procedures, honor a contract between users and organization outlining mutual responsibilities for secure access, and integrate utilitarian, deontological, virtue ethics, contractarian, and care ethics perspectives to address ethic dimensions.

Question 10

Develop a specific security policy statement for ID/Authentication.

Policy Statement: All users must authenticate with multi-factor authentication (MFA) to access systems of the organization. This includes a combination of: passwords, biometric verification including face and fingureprint, and a secondary device-based confirmation. MFA combines at least two of the these verification methods:

1. Something You Know: A strong password.
2. Something You Have: A hardware token or mobile device authentication app.
3. Something You Are: Biometric verification.

Furthermore:

1. Password Requirements:
    - Minimum length of 12 characters.
    - Must include alphanumeric and special characters.
    - Updated every 90 days.
2. Biometric Data:
    - Stored securely and encrypted.
    - Used exclusively for authentication purposes without being shared.
3. Hardware Tokens:
    - Issued and managed by the IT department.
    - Users must report lost or stolen tokens immediately.
4. Security Awareness Training:
    - Mandatory training sessions.
    - Focus on recognizing phishing attempts, secure password practices, safe use of mobile/personal devices.

Rationale: MFA enhances security by reducing risk of unauthorized access. This policy conforms with ethical theories, making sure user data protection (deontology), maximizing security benefits (utilitarianism), fostering trust (virtue ethics), respecting social contracts (contractarianism), caring for user safety (care ethics).

https://app.originality.ai/share/zsck2ol3it6vxhw9

Academic Integrity Pledge

"This work complies with JMU honor code. I did not give or receive unauthorized help on this assignment."