NOTES

YOUR FACE IS A COMMODITY, FIERCELY CONTRACT ACCORDINGLY: REGULATING THE CAPITALIZATION OF FACIAL RECOGNITION TECHNOLOGY THROUGH CONTRACT LAW

Y. AMY CHEN*

ABSTRACT

Many believe that models, the likes of Candice Swanepoel and Sara Sampaio, are the only ones that can contract the image of their face for proceeds or benefits. However, with the rise of supply and demand in uses for facial recognition technology, by companies providing the technology and consumers using it, biometric data, specifically facial recognition technology data has become a tradeable commodity. Unfortunately, state regulations are weak in their attempts to curb advantageous private companies from taking advantage of consumers' data and federal regulation is virtually nonexistent. Consumers, without appreciating the dangers of consenting to use of their facial recognition data and the value that such biometric data has, readily sign off rights to their facial data for minor conveniences. This Note discusses where regulations fall short and where improvements can be made to protect consumers.

INTRODUCTION

Each year technology advances, disrupting our way of life. It pushes the boundaries of settled law and forces the question of whether our current portfolio of rules and regulations allow for technology to cleanly fit into the boundaries of precedents courts set forward. The newest technology to peak public interest is facial recognition technology (FRT). Since Woodrow Wilson Bledsoe in the 1960s, who most consider the father of facial recognition, began measuring the relative coordinate locations of facial features, the technology

* J.D. Candidate, University of Notre Dame Law School, 2020. I would like to extend my gratitude to Professor Mark McKenna for his mentorship in the full process it took to complete this Note, as well as his expertise in privacy law. I would also like to thank Professor Mary Ellen O'Connell for her helpful thoughts overall and expertise in contract law. Additionally, I would like to extend gratitude to Professor Timothy Flanagan for sharing his experience and expertise in information technology law and Professor Patrick Flynn for his expertise in facial recognition technology. Thank you to Professor Woodrow Hartzog for our discussion and inspiration for the topic. Lastly, I would like to thank the editors of the *Notre Dame Journal of Law, Ethics and Public Policy* for their careful edits. All errors and opinions are my own.

has become more robust in accuracy.[1] In addition, its use has expanded both in private use, such as at the Super Bowl XXXV or by Facebook's photograph identity tagging, and in public sector use, such as in identifying terrorists.[2] Although there is much to be concerned about with public use of FRT, this Note focuses on private sector capitalization of FRT.

Technology industry front-runners, Apple and Microsoft, embrace the technology, however, to varying degrees shown by the juxtaposition on the stances and actions they have taken revolving FRT. In 2018, Apple retired its Touch ID fingerprint biometric scanners in all new models of their iPhone products.[3] Apple touts that Face ID "revolutionizes authentication"; however, it is silent on any dangers or concerns.[4] Meanwhile, Microsoft, also owning its own proprietary FRT, has publicly asked for government regulation on the technology.[5] Most recently, Amazon has joined the discussion siding with Microsoft on more regulation on FRTs.[6] However, this stance seems to come as a response to negative publicity regarding its shareholders' pressures and disapproval of the company selling its Rekognition FRT to the United States Government.[7]

---

1. *See* Jesse Davis West, *A Brief History of Face Recognition*, FACEFIRST (Aug. 1, 2017), https://www.facefirst.com/blog/brief-history-of-face-recognition-software.

2. *See id.*

3. *See iPhone*, APPLE, https://www.apple.com/iphone (last visited Jan. 20, 2019) (noting that the iPhone XS and iPhone XR models only include facial authentication with Face ID); *see also* Mark Sullivan, *The iPhone X Gave Up on Touch ID, but Fingerprint Sensors Have a Future*, FAST COMPANY: TECH FORECAST (Dec. 15, 2017), https://www.fastcompany.com/40508767/the-iphone-x-gave-up-on-touch-id-but-fingerprint-sensors-have-a-future. Conversely, note that Apple has reportedly filed patents for fingerprint scanning technology under the surface of a screen, no longer needing a designated scanning location, suggesting that they may reembrace fingerprint authentication in conjunction with FRT. *See* Gordon Kelly, *Apple Plans Touch ID iPhone Comeback*, FORBES (Aug. 19, 2018, 9:20 PM), https://www.forbes.com/sites/gordonkelly/2018/08/19/apple-iphone-x-plus-se2-x2-upgrade-release-date-price-cost-face-id-touch-id/#7f99609647ab.

4. *See The Future Is Here: iPhone X*, APPLE (Sept. 12, 2017), https://www.apple.com/newsroom/2017/09/the-future-is-here-iphone-x.

5. *See* Brad Smith, *Facial Recognition Technology: The Need for Public Regulation and Corporate Responsibility*, MICROSOFT: MICROSOFT ON ISSUES (July 13, 2018), https://blogs.microsoft.com/on-the-issues/2018/07/13/facial-recognition-technology-the-need-for-public-regulation-and-corporate-responsibility ("This in fact is what we believe is needed today – a government initiative to regulate the proper use of facial recognition technology, informed first by a bipartisan and expert commission.").

6. *See* Michael Punke, *Some Thoughts on Facial Recognition Legislation*, AMAZON WEB SERVS.: AWS MACHINE LEARNING BLOG (Feb. 7, 2019), https://aws.amazon.com/blogs/machine-learning/some-thoughts-on-facial-recognition-legislation/?linkCode=w50&tag=w050b-20&imprToken=ZQf4J1gn1cpL8z3BEPC2jg&slotNum=0.

7. *See* Charlie Osborne, *US Regulators Dash Amazon Hopes to Stop Investor Vote on Gov't Facial Recognition Tech Sales*, ZDNET (Apr. 9, 2019, 11:03 AM), https://www.zdnet.com/article/us-regulators-block-amazon-attempt-to-stop-investor-vote-on-government-facial-recognition-tech-sale/.

Consumers, many of whom have yet to fully appreciate the potential dangers of FRT data, more than readily subscribe to the use of FRT for small gains in day-to-day convenience, unproportionate to the value in FRT data they are licensing to companies. The ideal case to analyze such a transaction of FRT data for benefits is Delta's new boarding process that dispenses of physical boarding passes and instead uses FRT to authenticate passengers during the boarding process.[8] When the technology launched November of 2018 in Hartsfield-Jackson Atlanta International Airport's (ATL) Terminal F, twenty-five thousand customers chose to use the FRT boarding process; less than two percent opted out of the optional process.[9] Delta claims that once opted-in,[10] consumers simply must approach the camera and board;[11] this eliminates an equally simple task of locating a boarding pass and scanning the pass for entry, saving only a negligible amount of time of the aggregate boarding process.[12] The FRT boarding registration numbers demonstrate a clear embracement and possible normalization of the technology by consumers without any evidence that they realize the contractual and other privacy ramifications of trading off access to one's own valuable facial features for an ounce of convenience. Given that FRT is still a new development in the technology industry, the full extent of its commercial use and capabilities remains largely unknown.[13] How can regulators protect consumers who do not understand the full breadth of what they are giving up? What does an ideal agreement look like when companies seem to have a large bargaining power, yet consumers unknowingly hold the gem of biometric data[14] in their hands?

Delta's FRT boarding service is not yet available in Illinois,[15] likely because the state has what is considered the most robust of the currently enacted state regulations on biometric data through its Biometric Information Privacy

---

8. *See* Kathryn Steele, *Delta Unveils First Biometric Terminal in U.S. in Atlanta; Next Stop: Detroit*, DELTA: NEWS HUB (Nov. 29, 2018, 6:00 AM), https://news.delta.com/delta-unveils-first-biometric-terminal-us-atlanta-next-stop-detroit.

9. *Id.*

10. Full details of how to register or opt-out to the process are unavailable. Also unavailable are any details on the contract consumers are shown when registering.

11. *See* Kathryn Steele, *Delta Tests Facial Recognition Boarding, Tops Off Year of Innovation in ATL*, DELTA: NEWS HUB (Dec. 15, 2017, 2:00 PM), https://news.delta.com/delta-tests-facial-recognition-boarding-tops-year-innovation-atl.

12. *See* Zack Whittaker, *Delta to Start Scanning Faces at Airport Check-in*, TECHCRUNCH (Sept. 20, 2018, 3:00 PM), https://techcrunch.com/2018/09/20/delta-to-start-scanning-faces-at-airport-check-in/ (noting that the process only decreases a few minutes off each flight).

13. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-15-621, FACIAL RECOGNITION TECHNOLOGY: COMMERCIAL USES, PRIVACY ISSUES, AND APPLICABLE FEDERAL LAW 1, 6 (2015).

14. The term "biometric data," as used in this Note, subsumes facial recognition data.

15. Kathryn Steele, *Delta Expands Optional Facial Recognition Boarding to New Airports, More Customers*, DELTA: NEWS HUB (Dec. 8, 2019, 1:39 AM), https://news.delta.com/delta-expands-optional-facial-recognition-boarding-new-airports-more-customers (stating that FRT boarding is only available at the following airports: Hartsfield-Jackson Atlanta International Airport, Minneapolis-Saint Paul International Airport, and Salt Lake City International Airport).

Act (BIPA).[16] Thus, the BIPA provides insight on how current regulation and the current technology landscape interplay. Although the BIPA leads the way in giving consumers more protection of their biometric data, its clear pitfall lies in its notice and consent model.[17] Simply put, companies need only to provide notice to consumers of how biometric data is to be used and obtain written consent from the consumer. Thus, a consumer may legally be notified, but a cursory glance on the more mature law revolving online contracts, such as clickwrap terms and agreements, show how this model falls short of meaningfully notifying consumers of the legal contract they are entering.

Thus, as FRT continues to develop and integrate itself into the world, it is not difficult to imagine a hypothetical scenario where Delta's facial recognition boarding is bounded by a BIPA-like regulation. In this scenario, two main concerns arise revolving the lack of adequate consumer protection: (1) consumers are too naïve in evaluating the relative consideration in the facial recognition data they are giving up and the convenience they are receiving, creating a concerning contracting dynamic; and (2) the current bare notice and consent model around contracting facial recognition data is insufficient to force consumers to appreciate the legal consequences of the transaction.

Part I of this Note discusses shortly how FRT works and the pros and cons of the technology, overall focusing on how facial recognition data concerns differ from other similarly situated biometric data. Then, Part II analyzes the legal landscape regarding laws that directly govern FRT and relevant contract law and behavioral economics. Part II.A analyzes the current regulatory landscape on FRT and use of facial recognition data, or lack thereof. Part II.B analyzes relevant traditional contracting economics, thus acknowledging the aforementioned concern of the contracting dynamic between the private companies and consumers. Part II.B also analyzes the analogous and more settled legal landscape around online contracting of terms and conditions, focusing on the concerns of a notice and consent regulatory model. Finally, Part III takes these two concerns and proposes a solution to accompany a BIPA-like regulation through a model agreement and default provisions as well as a super-consent requirement to regulations.

I. FACIAL RECOGNITION TECHNOLOGY

A. A Brief, Technical Overview

Biometrics is the measuring of physical or behavioral traits and then using that information to provide some form of value, such as security authentication or determining identity.[18] Facial recognition is just one of many biometrics; others include physical biometrics such as facial recognition, iris recognition,

16. *See infra* Section II.A.1.b.

17. *See infra* note 86 and accompanying text.

18. *See* Gaurav Aggarwal et al., *Physics-Based Revocable Face Recognition*, *in* 2008 IEEE INTERNATIONAL CONFERENCE ON ACOUSTICS, SPEECH AND SIGNAL PROCESSING 5232, 5232 (2008).

and fingerprint recognition and behavioral biometrics, including walking patterns, gestures, and voice recognition.[19]

Looking more closely at how FRT works, there are four components to an FRT system: (1) a camera to capture an image; (2) an algorithm to create a faceprint; (3) a database of stored images; and (4) an algorithm to compare the captured image to the database of images or a single image in the database.[20] A faceprint, similar to a fingerprint, is how a system's code recognizes and measures an individual's unique facial features.[21] Each FRT system can use a variety of methods or combination of methods to create a faceprint which can then be used to match back to a database which stores references from multiple faceprints linked to an individual's identity.[22] For example, Apple's Face ID creates a faceprint by projecting over thirty thousand invisible dots which are used to map out and analyze an individual's face; Apple also stores an infrared image of the face.[23] The faceprint is then converted to a mathematical representation and encrypted with a key that only Secure Enclave[24] has possession of.[25] Compare thirty thousand dots to the technology used in the 1970s where only twenty-one markers were used,[26] and there is no surprise that accuracy has increased over time with advancements in technological capabilities.[27]

Some argue that the dangers that come with FRT may not be that different from those that come from the biometric technology that is already out being used.[28] However, that view is misguided; it is clouded by the foundational

---

19. *See The Future of Biometrics Technology: Convenience or Privacy?*, THOMSON REUTERS: DATA PRIVACY (June 2, 2017), https://blogs.thomsonreuters.com/answerson/biometrics-technology-convenience-data-privacy.

20. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-15-621, FACIAL RECOGNITION TECHNOLOGY: COMMERCIAL USES, PRIVACY ISSUES, AND APPLICABLE FEDERAL LAW 3 (2015).

21. *See id.* at 3 n.5 ("A faceprint or facial template is essentially a digital code that a facial recognition algorithm creates from an image. Faceprints generally are unique to a particular company because different companies use different facial recognition algorithms, according to industry sources.").

22. *See id.* at 4.

23. *See About Face ID Advanced Technology*, APPLE (Sept. 19, 2019), https://support.apple.com/en-us/HT208108.

24. *See id.* Secure Enclave is Apple's hardware-based key manager in charge of Apple products' security framework that handles encryption. Because it is hardware based, there is no transfer of keys between devices which is fundamental to its security function. *See Storing Keys in the Secure Enclave*, APPLE: DEVELOPER, https://developer.apple.com/documentation/security/certificate_key_and_trust_services/keys/storing_keys_in_the_secure_enclave (last visited Mar. 12, 2019). Note that there are no additional details to form an accurate conclusion on whether this encryption is cancelable and thus qualifies as a revocable biometric, *infra* Section I.A.C.

25. *See About Face ID Advanced Technology*, *supra* note 23.

26. *See* West, *supra* note 1.

27. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-15-621, FACIAL RECOGNITION TECHNOLOGY: COMMERCIAL USES, PRIVACY ISSUES, AND APPLICABLE FEDERAL LAW 5 (2015).

28. *See id.* at 17–19.

similarities of biometric data. With biometric data use becoming so widespread, such as smartphone fingerprint scanning[29] and even commercialization of iris scanning identity verification,[30] experts warn that FRT poses a unique threat to the population[31] and thus a threat to consumers of its commercialization. Faces are central to our identity.[32] Not only are faces primary identifiers, but society has put an emphasis on faces in social interaction because faces show emotion and attentiveness.[33] Our experiences have taught us that faces are important, and yet this important data, unlike alphanumeric passwords, cannot be hidden.[34] They are public and easily captured without notification and consent, unlike iris or fingerprint data.[35] These concerns are compounded due to the already existing foundation of data collected and existing use of necessary technology that is needed for FRT system to function, and thus the environment already exists for abuse of the technology, such as surveillance creep; drivers' licenses, criminal mugshots, and passport photos provide the databases of name to faceprint while security cameras are the technology that provide the means for capturing and tracking images.[36] But to truly understand why there are such polarizing views on the use of FRT, it is important to understand the arguments on the benefits and costs of the use of the technology.

B. The Benefits

Most of the benefits that proponents of FRT focus on are in relation to safety and security; this can range from economic necessity, such as casinos banning known cheaters through FRT identification,[37] to personal security measures, such as identity validation. For consumers, personal security is the most intriguing benefit, and what makes FRT so valuable is that it can be used

29. *See Global Penetration of Smartphones with Fingerprint Sensors 2014-2018*, STATISTA (Jan. 5, 2016), https://www.statista.com/statistics/522058/global-smartphone-fingerprint-penetration (showing the penetration of fingerprint sensors in the smartphone market growing from 19% in 2014 to 67% in 2018).

30. *See* CLEAR, https://www.clearme.com (last visited Feb. 8, 2019) (noting that Clear uses both fingerprint and iris scanning at over 40 airports across the United States).

31. *See* Woodrow Hartzog & Evan Selinger, *Facial Recognition Is the Perfect Tool for Oppression*, MEDIUM (Aug. 2, 2018), https://medium.com/s/story/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66.

32. *See id.*

33. *See* David A. Leopold & Gillian Rhodes, *A Comparative View of Face Perception*, 124 J. COMP. PSYCHOL. 233, 233 (2010) ("[A]s a species we are constantly, almost obsessively, monitoring each other's faces, paying close attention to subtle details that can give some insight into the emotional state, level of engagement, or object of attention of our associates. Fluency with faces offers great social advantages . . . .").

34. *See* Hartzog & Selinger, *supra* note 31.

35. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-15-621, FACIAL RECOGNITION TECHNOLOGY: COMMERCIAL USES, PRIVACY ISSUES, AND APPLICABLE FEDERAL LAW 15 (2015).

36. *See* Hartzog & Selinger, *supra* note 31.

37. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-15-621, FACIAL RECOGNITION TECHNOLOGY: COMMERCIAL USES, PRIVACY ISSUES, AND APPLICABLE FEDERAL LAW 8 (2015).

in lieu of passwords and thus no password management is necessary.[38] Instead of having to remember and create secure passwords for bank accounts, users can simply validate their identity using their unique facial features. Unlike passwords, your face cannot be as easily stolen or used by others,[39] but this does not mean that the technology cannot be fooled or hacked.[40] However, although an FRT's function is usually focused on the surface in what it does for security, the true benefit or marketability of the technology to everyday consumers is found in the added value of convenience. As previously mentioned, Delta is using the technology for a quicker boarding process.[41] Facebook uses it to easily tag photos.[42] Apple uses it to manage and categorize photos, grouping photos with the same individuals together.[43] There is demand for small conveniences and customization; where there is demand, there are businesses ready to supply and rake in the revenue.

For those on the FRT supply and data-collection side, in addition to convenience, FRT adds value through its tracking capabilities. Again, much of this is generally understood as a safety and security benefit when looking at FRT use in the public sector; FRT tracking can assist in domestic crime solving: FRT could pair with already existing social media intelligence (SOCMINT) to supplement tools for domestic criminal law[44] or it could increase the efficiency of an all-points bulletin (APB)[45] by decreasing the manual labor of locating wanted criminals.[46] On a larger scale, the technology is being considered for use by federal agencies in regulating travel in antiterrorism efforts.[47] But the

---

38. *See id.* at 9.

39. *See* Aggarwal et al., *supra* note 18, at 5232.

40. *See* Andy Greenberg, *Hackers Say They've Broken Face ID a Week After iPhone X Release*, WIRED (Nov. 12, 2017, 6:44 PM), https://www.wired.com/story/hackers-say-broke-face-id-security/.

41. *See* Lucas Laursen, *Delta Is Rolling Out Facial Recognition Check-in That It Says Will Save You 9 Minutes Per Flight*, FORTUNE (Sep. 21, 2018, 7:05 AM), http://fortune.com/2018/09/21/delta-air-lines-atlanta-airport-facial-recognition.

42. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-15-621, FACIAL RECOGNITION TECHNOLOGY: COMMERCIAL USES, PRIVACY ISSUES, AND APPLICABLE FEDERAL LAW 11 (2015).

43. *See About People in Photos on Your iPhone, iPad, or iPod Touch*, APPLE, https://support.apple.com/en-us/HT207103 (last visited Feb. 8, 2019).

44. *See* Laura K. Donohue, *The Dawn of Social Intelligence (SOCINT)*, 63 DRAKE L. REV. 1061 (2015).

45. An APB, or all-points bulletin, is "a general bulletin broadcast to alert law-enforcement officers over a wide area that someone (such as a suspect) or something (such as a vehicle) is being actively sought in connection with a crime." *All-points Bulletin*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/all-points%20bulletin (last visited Feb. 8, 2019).

46. *See* Laursen, *supra* note 41 ("Last month, officials at Dulles Airport in Washington, D.C. arrested a man using facial recognition. And the U.S. Department of Homeland Security wrote last year in its Privacy Impact Assessment Update that international travelers to or from the U.S. cannot opt out of biometric identification.").

47. Using facial recognition, the United States Customs and Border Protection identified a Republic of Congo citizen attempting to enter the United States illegally as a French national. *See* Shannon Liao, *New Facial Recognition System Catches First Imposter at US Airport*, VERGE (Aug.

core functionality and how it differs from other biometric technologies for companies is how easily humans can be tracked without knowledge and consent. Currently companies are already tracking consumers' virtual movements through cookies or virtual tracking devices and utilizing that data for targeted advertisements.[48] Through FRT, companies would be able to further customize their sales approach by tying consumer's online presence to their offline presence, opening the door to incredibly valuable behavioral data such as shopping mannerisms.[49] Retailers are also hoping to use the technology to deputize themselves in preventing shoplifting.[50] The demand in the private sector is just as evident as it is in the public sector.

C. The Costs

And yet, for every benefit there is an equal and opposite cost of the technology. Consumers are not foreign to intentional data breach and abuse; two notable examples include the U.S. Office of Personnel Management (OPM) data hack by a Chinese national back in 2015 which affected United States government employees[51] while the Equifax breach in 2017 affected 145.5 million customers.[52] Biometric data once compromised has no recourse. Unlike passwords that can be changed, a fingerprint, an iris, a face are all immutable

---

24, 2018, 1:41 PM), https://www.theverge.com/2018/8/24/17778736/facial-recognition-washington-airport-immigration-biometric-exit. This technology has already been deployed to multiple customs entry and exit points; however, the source notes that United States citizens are not required to use the service and can opt-out. *See Biometrics*, U.S. CUSTOMS & BORDER PROTECTION, https://www.cbp.gov/travel/biometrics#How-it-works (last visited Feb. 8, 2019); Dami Lee, *TSA Lays Out Plans to Use Facial Recognition for Domestic Flights*, VERGE (Oct. 15, 2018, 3:35 PM), https://www.theverge.com/2018/10/15/17979688/tsa-precheck-facial-recognition-airport-cbp-biometric-exit (discussing TSA's plan for using FRT in domestic travel).

48. *See* Laura Sydell, *Smart Cookies Put Targeted Online Ads on the Rise*, NPR: TECH. (Oct. 5, 2010, 11:46 AM), https://www.npr.org/templates/story/story.php?storyId=130349989 ("'You're talking about a commercial system that's a digital dossier about your innermost secrets, concerns and personal matters,' [Jeff] Chester says.").

49. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-15-621, FACIAL RECOGNITION TECHNOLOGY: COMMERCIAL USES, PRIVACY ISSUES, AND APPLICABLE FEDERAL LAW 9 (2015).

50. *See* Leticia Miranda, *Thousands of Stores Will Soon Use Facial Recognition, and They Won't Need Your Consent*, BUZZFEED NEWS (Aug. 17, 2018, 10:28 AM), https://www.buzzfeednews.com/article/leticiamiranda/retail-companies-are-testing-out-facial-recognition-at.

51. *See* Evan Perez, *FBI Arrests Chinese National Connected to Malware Used in OPM Data Breach*, CNN: POL. (Aug. 24, 2017, 6:29 PM), https://www-m.cnn.com/2017/08/24/politics/fbi-arrests-chinese-national-in-opm-data-breach/index.html?r=https%3A%2F%2Fwww.google.com%2F.

52. *See* Donna Borak & Kathryn Vasel, *The Equifax Hack Could Be Worse than We Thought*, CNN: MONEY (Feb. 10, 2018, 10:43 AM), https://money.cnn.com/2018/02/09/pf/equifax-hack-senate-disclosure/index.html; *see also* Selena Larson, *The Hacks That Left Us Exposed in 2017*, CNN: BUS. (Dec. 20, 2017, 9:11 AM), https://money.cnn.com/2017/12/18/technology/biggest-cyberattacks-of-the-year/index.html?iid=EL (noting other high-profile data breaches in 2017).

features. The once praised feature that allowed biometric data to trump traditional passwords in its seemingly unbreakable[53] authenticity has become its biggest flaw. One's faceprint is more susceptible to being stolen compared to other biometric data because we wear our faces in public, unhidden, and one's faceprint can easily be captured from a distance without notice.[54]

However, it is important to note that research and development is being conducted on revocable biometrics.[55] Revocable biometrics combines a biometric-based authentication system with a user-specific private key, which can be cancelled and replaced when compromised. This user-specific key is used to encrypt the faceprint image, essentially distorting it, before storing it in a database. However, this technology is limited in its use in large-scale databases; because the stored image is encrypted, the system cannot learn to adjust to small differences when authenticating, and thus is sensitive to noise,[56] rendering the method commercially unviable. To combat this deficiency, a 3D or physics-based model of encryption and decryption is being developed, but there is little evidence of the technology being used commercially.[57] In addition, research warns that "though it is impossible for an adversary to get the original image back from just a transformed image and the corresponding key, the transform is invertible if he/she has access to the exact distortion algorithm used to obtain the transformed images."[58]

Further, consider the effect that FRT has on tracking and surveillance,[59] keeping in mind that it was previously discussed as a benefit. Consider the amplification of surveillance capitalism,[60] again mentioned before in the context of value to business marketing. It is shocking to imagine the potential damage for intentional abuse of FRT data. The foundation of the concern in the private sector is that consumers are largely unappreciative of the dangers that come

---

53. Apple's spoof detection, *see* Andy Greenberg, *We Tried Really Hard to Beat Face ID—and Failed (So Far)*, WIRED (Nov. 3, 2017, 7:00 AM), https://www.wired.com/story/tried-to-beat-face-id-and-failed-so-far, was inadvertently "hacked" by a 10-year-old who had enough familial similarities to his mother and thus unlocked her phone which stored her faceprint. *See* Kirsten Korosec, *Mom's iPhone X Unlocked by 10-Year-Old's Face*, FORTUNE (Nov. 14, 2017, 1:47 PM), http://fortune.com/2017/11/14/apple-iphone-x-face-id-unlocked. The article notes that his face is not similar enough to fall under the "twins" exception that can fool Apple's thirty thousand markers. *Id*.

54. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-15-621, FACIAL RECOGNITION TECHNOLOGY: COMMERCIAL USES, PRIVACY ISSUES, AND APPLICABLE FEDERAL LAW 15 (2015).

55. *See* Aggarwal et al., *supra* note 18.

56. *See id.*

57. Note that although Apple's Secure Enclave hardware-based encryption uses a similar encryption and decryption process, *see Storing Keys in the Secure Enclave*, *supra* note 24, Apple devices do not store a large database of faceprints which is the main concern of the commercial viability in this study. Aggarwal et al., *supra* note 18.

58. Aggarwal et al., *supra* note 18, at 5235.

59. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-15-621, FACIAL RECOGNITION TECHNOLOGY: COMMERCIAL USES, PRIVACY ISSUES, AND APPLICABLE FEDERAL LAW 14 (2015).

60. *See* Hartzog & Selinger, *supra* note 31.

from contracting away privacy rights with respect to FRTs. Technology industry giants who are saturating the market with FRTs are normalizing the consumers to the technology without adequately educating consumers of the costs. This issue is further compounded by the fact that our faces are public but are still subject to privacy laws.[61] Thus, privacy law becomes something of a misnomer in consumers' minds given that the general rule by courts states that "there can be no privacy in that which is already public."[62] Yes, faces are public and seen by the population every day, but the danger in FRTs lies in the computer processing. Humans can only remember a finite amount of faces creating natural, biologically limited obscurity zones.[63] Obscurity is the idea that, due to transaction costs, information is in a sense out of reach even though it may be technically public.[64] This solidifies the theory that people have privacy rights in faces even though they are technically public, but computers have unlimited processing power; FRTs are able to pick up more information than the human brain and process it more aggressively than humans are able to.[65] Therefore, that natural limit that protected anonymity, that supported privacy rights for faces, is no longer a safeguard.[66]

FRTs are not perfect. Just as any technology available, it is only as smart as the person coding the system and processes.[67] And yet, the conclusions drawn by FRTs are treated as the truth leading to constitutional concerns.[68] Meanwhile data supports that because of the way the authentication image is captured, it is less accurate than other biometric means of identification.[69] Clare Garvie asks, "What happens if a system like this gets it wrong? A mistake by a video-based surveillance system may mean an innocent person is followed, investigated, and maybe even arrested and charged for a crime he or she didn't commit."[70] The same question can be asked regarding commercialization of the technology. What happens if a video-based surveillance system records the wrong person, one who has not consented or contracted away his or her rights? This weakness is very real as FRTs are known to have difficulty with faces that

61. *See* Woodrow Hartzog, *The Public Information Fallacy*, 99 B.U. L. REV. 459 (2019).

62. *Id.* at 461 (quoting Gill v. Hearst Publ'g Co., 253 P.2d 441, 444 (Cal. 1953)).

63. *See* Hartzog & Selinger, *supra* note 31.

64. *See* Evan Selinger & Woodrow Hartzog, *Obscurity and Privacy*, *in* SPACES FOR THE FUTURE: A COMPANION TO PHILOSOPHY OF TECHNOLOGY 119 (Joseph C. Pitt & Ashley Shew eds., 2017).

65. *See id.*

66. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-15-621, FACIAL RECOGNITION TECHNOLOGY: COMMERCIAL USES, PRIVACY ISSUES, AND APPLICABLE FEDERAL LAW 13 (2015).

67. *See* Christian Chessman, *A "Source" of Error: Computer Code, Criminal Defendants, and the Constitution*, 105 CALIF. L. REV. 179, 181 (2017) (noting that although a computer follows commands perfectly, the commands come from a human programmer).

68. *See id.*

69. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-15-621, FACIAL RECOGNITION TECHNOLOGY: COMMERCIAL USES, PRIVACY ISSUES, AND APPLICABLE FEDERAL LAW 17 (2015).

70. Hartzog & Selinger, *supra* note 31.

are not Caucasian.[71] Unintentional biases of FRT systems is one issue, but it also lends itself to concerns on the intentional uses of bias. Because of the way FRTs function as opposed to other biometrics, they allow for abuse that compromises civil rights. FRT data has the ability to be used in a way to classify people and, in its ugliest form, to discriminate against certain types people.[72]

II. LAWS, REGULATION, AND CONTRACT THEORY REGARDING FACIAL RECOGNITION TECHNOLOGY

A. Current Laws and Regulation

Knowledge and consent are major concerns for FRTs as opposed to other biometric authentication systems because a faceprint can be taken from afar and without notice.[73] The Computer and Communications Industry Association stated that the technology should be transparent and give individuals a choice to opt out.[74] Thus it is no surprise that statutes on biometric data protection focus largely on a notice and consent model.[75] Privacy law protections focus on self-management by consumers, allowing them to evaluate whether to consent or not to providing information about themselves.[76] Yet, it has been proven that consumers are unable to adequately analyze these evaluations.[77] So why then do laws still focus on simple notice and consent models?

1. Weak but Existing State Law

a. Texas and Washington

Texas law governs the capture and use of biometric identifiers, which includes FRTs under the term "face geometry."[78] The statute states that capture of an individual's biometric identifier is not permitted for a commercial purpose

---

71. *See* Steve Lohr, *Facial Recognition Is Accurate, If You're a White Guy*, N.Y. TIMES (Feb. 9 2018), https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html; Tom Simonite, *How Coders Are Fighting Bias in Facial Recognition Software*, WIRED (Mar. 29, 2018, 7:00 AM), https://www.wired.com/story/how-coders-are-fighting-bias-in-facial-recognition-software.

72. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-15-621, FACIAL RECOGNITION TECHNOLOGY: COMMERCIAL USES, PRIVACY ISSUES, AND APPLICABLE FEDERAL LAW 17 (2015); Punke, *supra* note 6 ("Concerns have been raised about how facial recognition could be used to discriminate and violate civil rights.").

73. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-15-621, FACIAL RECOGNITION TECHNOLOGY: COMMERCIAL USES, PRIVACY ISSUES, AND APPLICABLE FEDERAL LAW 15 (2015).

74. *See id.*

75. *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 594 (2014) ("Even when statutes were passed, they often embraced the notice-and-choice approach.").

76. *See* Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1880 (2013).

77. *See id.* at 1880–81.

78. TEX. BUS. & COM. CODE ANN. § 503.001(a) (West 2017).

unless the individual is informed beforehand and consents. The statute also limits the ability to sell or transfer the data without consent with certain exceptions.[79] Texas law requires reasonable care in the storage of the data in the same or more protective manner as similar data[80] as well as destruction of the data within a year at maximum unless another law maintains otherwise, at which point the data can only be kept for a reasonable time.[81] The maximum civil penalty for a violation is $25,000 per violation.[82]

Washington's laws offer less protection although they retain the similar notice and consent structure for biometric data stored for commercial purposes.[83] The State requires reasonable precautions to be taken with the storage and protection of the data, and the data cannot be retained for longer than reasonable, although the law is silent on any hard deadlines.[84] Note that Washington's law explicitly states that the notice and consent requirement of the statute does not apply to data collection for security purposes, thus creating a hole in protection.[85]

b. Illinois

Although still imperfectly based on a notice and consent model,[86] Illinois's law, the Biometric Information Privacy Act (BIPA), on biometric data is a step above both Texas's and Washington's laws. Illinois requires that private entities that possess biometric data publicly publish a retention schedule and guideline on destruction of the data it collects.[87] Illinois's law backs away from a reasonableness standard for retaining data, a vague standard that both Texas and Washington use, and sets a maximum limit on data retention on the earlier of when the purpose of the retention has been met or three years from the last interaction of the individual whose biometric data was collected.[88] The law also requires that data be protected as consistent with industry standards and at the same or higher protective measures as other confidential and sensitive information.[89]

As for remedies, the statute delineates damages based on the mens rea of the violation. For negligent violations of the BIPA, damages are the greater of liquidated damages of $1,000 or actual damages.[90] For reckless or intentional

79. *Id.* § 503.001(c)(1).

80. *Id.* § 503.001(c)(2).

81. *Id.* § 503.001(c)(3).

82. *Id.* § 503.001(d).

83. WASH. REV. CODE ANN. § 19.375.020 (LexisNexis 2018). Note that regulation for biometric identifiers for government agencies is regulated under *id.* § 40.26.020.

84. *Id.* § 19.375.020(4).

85. *Id.* § 19.375.020(7).

86. 740 ILL. COMP. STAT. ANN. 14/15(b) (LexisNexis 2019).

87. *Id.* 14/15(a).

88. *Id.*

89. *Id.* 14/15(e)(2).

90. *Id.* 14/20(1).

violations, damages are the greater of liquidated damages of $5,000 or actual damages.[91] Reasonable attorney's fees and injunctions may also be awarded depending on the case.[92]

The BIPA is also considered a more robust law due to the higher volume of cases showing the application and nuances of the law when enforced and further drawing the boundaries. *Rosenbach v. Six Flags Entertainment Corp.*,[93] *Rivera v. Google Inc.*,[94] and *In re Facebook Biometric Information Privacy Litigation*[95] are the trilogy of cases that have created the most impact on the law, and until the cases are fully settled though the judicial process, there may still be movement in the interpretation of the BIPA.

In *Rosenbach*, plaintiff's son went to defendant Six Flags's amusement park and was fingerprinted.[96] The fingerprint data was thus collected, then recorded, and further stored as part of a new security process for entry.[97] When plaintiff was notified of the biometric data collection, she sued the amusement park under the BIPA alleging that no written consent was provided and that the amusement park did not publish the requisite storage, usage, or destruction policy of the data.[98] Plaintiff admitted that no actual injury was suffered, but she would not have purchased admission for her son if she had known of the biometric data collection.[99] The court concluded that a BIPA plaintiff is required to do more than allege a technical violation of the Act, and that a defendant's failure to provide notice or obtain consent before collecting biometric data is not enough to meet the BIPA's "aggrieved by" standard.[100]

However, just recently the Supreme Court of Illinois overturned that decision.[101] After lengthy analysis of statutory interpretation, the court ultimately held that suffering actual damage is not necessary for a plaintiff to qualify as aggrieved.[102] The court further stated that the appellate court's prior holding, that the violation of the law was merely technical in nature, misunderstood the purpose of the legislation and the harm the law seeks to prevent.[103] This brings the case further in line with *In re Facebook*, where the

---

91. *Id.* 14/20(2).

92. *Id.* 14/20(3); *id.* 14/20(4).

93. Rosenbach v. Six Flags Entm't Corp., 2017 IL App. 2d 170317 (2017), *rev'd*, 129 N.E.3d 1197 (Ill. 2019).

94. Rivera v. Google Inc., 238 F. Supp. 3d 1088 (N.D. Ill. 2017).

95. *In re* Facebook Biometric Info. Privacy Litig., 185 F. Supp. 3d 1155 (N.D. Cal. 2016).

96. *Rosenbach*, 2017 IL App. 2d at ¶ 7.

97. *Id.*

98. *Rosenbach*, 2017 IL App. 2d at ¶ 10.

99. *Id.*

100. *Id.* at ¶ 23; 740 ILL. COMP. STAT. ANN. 14/20 (LexisNexis 2019) ("Any person aggrieved by a violation of this Act shall have a right of action . . . against an offending party.").

101. Note that the decision of this case is not final until the expiration of the twenty-one-day petition for rehearing period.

102. Rosenbach v. Six Flags Entm't Corp., 129 N.E.3d 1197, 1205 (Ill. 2019).

103. *Id.* at 1206.

court held that the BIPA codifies a right of privacy with regard to personal biometric information, and that a violation of that right is sufficient for a cause of action under the BIPA.[104]

In *Rivera*, the court adjudicated two similar cases against Google where a Google Droid device was used to take a picture of both plaintiffs, Rivera and Weiss, and the images were subsequently uploaded to Google's cloud-based image service.[105] Google then scanned and created faceprints of the plaintiffs which was then used to identify them in photos and group them together.[106] Defendant, Google, attempted to dismiss the claims, stating that the issue was the use of the plaintiffs' photographs and information from photographs is not within the BIPA's protection, thus the plaintiffs failed to state a claim.[107] The court, however, held that the BIPA does not dictate how biometric measurements must be obtained and thus defendant's motion to dismiss was denied.[108]

2. Lack of Direct Federal Law or Regulations

There is currently no federal privacy law that directly regulates commercial uses of FRTs, however, there may be law and or regulations that govern other industries that implicate limited usage of the data (e.g., healthcare, finance).[109] This lack of direct federal law on contracting of FRT data is concerning; consumer interests, when contracting away rights for FRT data, cannot sufficiently be protected just from positive externalities of other industries' laws due to the aforementioned nuances of biometric data, and further the elevated damage that FRT data abuse can lead to. Many organizations and groups have proposed possible guidelines for regulations in this field: National Telecommunications and Information Administration's (NTIA) multi-stakeholder process for facial recognition; International Biometrics & Identification Association's *Privacy Best Practice Recommendations for Commercial Biometric Use*; ACLU's *An Ethical Framework for Facial Recognition*; Federal Trade Commission's October 2012 staff report and Face Facts Forum; and stakeholders and advocates for privacy

> These procedural protections "are particularly crucial in our digital world . . . ." When a private entity fails to adhere to the statutory procedures, as defendants are alleged to have done here, "the right of the individual to maintain [his or] her biometric privacy vanishes into thin air. The precise harm the Illinois legislature sought to prevent is then realized." This is no mere "technicality." The injury is real and significant.

Id. (alteration in original) (citations omitted) (quoting Patel v. Facebook Inc., 290 F. Supp. 3d 948, 954 (N.D. Cal. 2018)).

104. *In re* Facebook Biometric Info. Privacy Litig., 185 F. Supp. 3d 1155 (N.D. Cal. 2016).

105. Rivera v. Google Inc., 238 F. Supp. 3d 1088, 1090–91 (N.D. Ill. 2017).

106. *Id.* at 1090–91.

107. *Id.* at 1090–92.

108. *Id.* at 1095.

109. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-15-621, FACIAL RECOGNITION TECHNOLOGY: COMMERCIAL USES, PRIVACY ISSUES, AND APPLICABLE FEDERAL LAW 28–31 (2015).

by design.[110] However, Congress may be finally ready to act.[111] Senator Roy Blunt sponsored the Commercial Facial Recognition Privacy Act of 2019 bill, Senate Bill 847.[112] However, Senate Bill 847 still follows a simple notice and consent model,[113] but it does encourage some information sharing from the commercial data collector to the consumer; companies must provide "where the end user can find more information about the use of facial recognition technology by the controller"[114] and provide "documentation that includes general information that explains the capabilities and limitations of the facial recognition technology in terms that end users are able to understand."[115] This protection would be a step in the right direction, potentially resolving the lack of information consumers have, but it does not fully address concerns such as consumers not fully reading the information provided in online contracts.[116]

B. Economics and Theory of Contract Law: Traditional Contracts and Online Contracts

1. Exceptions to the Freedom of Contract: Terms and Consideration

Contract law has been described with the term "freedom to contract" meaning that the parties are free to contract as long as the government has not restricted the subject matter of the contract[117] and courts have not refused to enforce it.[118] The growing trend of limitations to the freedom of contract seems to focus on limitation of the terms, which can take the form of immutable or default provisions, and regulation on the contracting process, such as focusing on relative consideration or formalities. Restrictions to the freedom of contract

110. *See id.* at 19–25.

111. *See* Davey Alba & Lissandra Villa, *As Concerns Over Facial Recognition Grow, Members of Congress Are Considering Their Next Move*, BUZZFEED NEWS (Feb. 20, 2019, 3:24 PM), https://www.buzzfeednews.com/article/daveyalba/house-oversight-committee-hearing-facial-recognition.

112. Commercial Facial Recognition Privacy Act of 2019, S. 847, 116th Cong. (2019) (introduced into Congress March 14, 2019 and as of April 19, 2019 it has been read twice and referred to the Committee on Commerce, Science, and Transportation).

113. *See id.* § 3(a)(1).

114. *Id.* § 3(a)(1)(B)(i).

115. *Id.* § 3(a)(1)(B)(ii).

116. *See* Caroline Cakebread, *You're Not Alone, No One Reads Terms of Service Agreements*, BUS. INSIDER (Nov. 15, 2017, 7:30 AM), https://www.businessinsider.com/deloitte-study-91-percent-agree-terms-of-service-without-reading-2017-11 (stating that 91% of consumers do not read legal terms and conditions before accepting and the language is too complex or long).

117. *See* Mark Pettit, Jr., *Freedom, Freedom of Contract, and the "Rise and Fall,"* 79 B.U. L. REV. 263, 280 (1999) ("Governmental action can restrict freedom of contract in two general ways. First, government can generate rules prohibiting certain types of private agreements. Second, government can refuse to enforce certain private contracts.").

118. *See id.* at 265.

can be categorized under two purposes: limitations to protect third parties or society and limitations to protect one or more contracting parties.[119]

In protecting third parties or the general public, limitations are generally put on types of contracts or certain terms that are void due to public policy.[120] Limitations to protect contracting parties include limitations preventing classes of people from contracting, a more absolute restriction controlling whether a contract can ultimately be formed between parties rather than the moderating the content. However, some argue that there is a trend moving away from and reducing restrictions, such as towards reducing the types of classes who are unable to enter into enforceable contracts.[121] Even those that believe the trend is facing the opposite direction, in creating more restrictions, can see that many of the laws are focused more on regulating the terms of contracts, not formation.[122] The most typical form of protection of individuals, rather than classes, focuses on the contracting process where the contract has become too one-sided, such as examining the relative bargaining power of the parties and the unconscionability doctrine as applied to the parties.[123]

Formalities of contracting can serve different functions, such as a cautionary function or a channeling function.[124] The cautionary function forces parties to consider their actions before contracting (e.g., through written requirements designed to slow down the contractual process).[125] The channeling function guides contracts by nudging parties to contract in the way that lawmakers prefer (e.g., increasing costs of contracting around defaults, thus leaving the default as the more efficient solution).[126]

Given that contract law has paternalistic roles, limiting the general rule of the freedom to contract, there is no surprise that contract regulation is based both on theories of human behavior and psychology.[127] Thus, understanding how default provisions, relative consideration, and formalities of the contract affect the parties' actions can draw a roadmap to more effective lawmaking.

a. Default Provisions and Its Effect on Information Disclosure

Immutable provisions, or immutable rules, are terms that parties cannot change by contractual agreements, thus protecting the interests of parties of the

119. *See id.* at 291.

120. *See id.* at 298.

121. *See id.* at 291–92.

122. *See id.* at 296.

123. *See id.* at 296–97 ("In many different ways, courts and legislatures have taken an increasingly active role in examining the fairness of the actions of contracting partners.").

124. *See* Ian Ayres & Robert Gertner, *Filling Gaps in Incomplete Contracts: An Economic Theory of Default Rules*, 99 YALE L.J. 87, 124 (1989).

125. *See id.*

126. *See id.* at 124–25.

127. *See* Craig Leonard Jackson, *Traditional Contract Theory: Old and New Attacks and Old and New Defenses*, 33 NEW ENG. L. REV. 365, 367 (1999).

contract and society's interest outside of the contract.[128] Immutable provisions are not impossible to circumnavigate, but they highly increase the transaction costs of doing so.[129] Therefore, immutable rules and default provisions are not two distinct measures, but rather they sit on opposite ends of a spectrum. Default provisions serve as a more flexible protective measure in regulating contracts for law makers and "[a]s the cost of contracting around a default rule becomes extremely large, the default starts to look [more] like an immutable rule."[130] All immutable rules, are simply default provisions with higher transaction costs. The question then is where on the scale of transaction costs sits the most effective provision to accomplish the protective goal lawmakers aim to achieve?[131] Do the concerns merit a more paternalistic measure? To apply default provisions effectively, those creating default provisions must understand the economics of contract law.[132] Contracts are incomplete for two general reasons: transaction costs and strategic withholding.[133] As a result, there are two approaches lawmakers take when determining how to set default provisions: (1) what the parties would have wanted and (2) strategic defaults or penalty defaults.[134]

Setting default provisions based on what the parties would have wanted implies economic efficiency; it therefore makes sense economically that the default provision be drafted to favor the party with the stronger bargaining power.[135] If drafting default provisions are contrary to this, giving the weaker party favor, the stronger party would likely distribute the cost to the weaker party regardless.[136] This is a fact of reality that outside of lawmaking the party with the stronger bargaining power has the advantage in the transaction. For example, in *The Original Great American Chocolate Chip Cookie Co. v. River Valley Cookies, Ltd.*,[137] Judge Posner upholds a termination clause that would allow a franchisor, the party with the stronger bargaining power, to terminate if

---

128. *See* Ayres & Gertner, *supra* note 124, at 87–88.

129. *See id.* at 121 (stating as an example the immutable rule that limited partnerships must have at least one general partner that has unlimited liability, however, some jurisdictions allow corporations to be a general partner, thus negating the requirement with a limited liability business entity).

130. *Id.*

131. *See id.* at 125–26 ("In essence, penalty defaults encourage, and 'strong' defaults discourage, contractual mutation. . . . [I]f parties attempt to contract around a default rule and fail, they will simply be bound by the default, whereas if parties attempt to contract around an immutable rule and fail, the law may choose to penalize . . . .").

132. *See id.* at 95 ("To set defaults efficiently, lawmakers must not only know what contracting parties want, but how many are likely to get it and at what cost.").

133. *See id.* at 92, 94.

134. *See id.* at 96–97.

135. *See* Omri Ben-Shahar, *A Bargaining Power Theory of Default Rules*, 109 COLUM. L. REV. 396 (2009).

136. *See id.* at 420–22.

137. The Original Great Am. Chocolate Chip Cookie Co. v. River Valley Cookies, Ltd., 970 F.2d 273 (7th Cir. 1992).

the franchisee commits misconduct, even if the misconduct does not amount to a level of breach of the contract.

> The idea that favoring one side or the other in a class of contract disputes can redistribute wealth is one of the most persistent illusions of judicial power. It comes from failing to consider the full consequences of legal decisions. Courts deciding contract cases cannot durably shift the balance of advantages to the weaker side of the market; they can only make contracts more costly to that side in the future, because franchisors will demand compensation for bearing onerous terms.[138]

But the question to bear in mind is will higher transaction costs slow down the contracting parties and thus force them to reassess the bargain in the transaction? Posner does not suggest how the weaker party will react, but it seems as if this would be so and could open another door to control how consumers contract.

Penalty defaults can also be drafted by lawmakers to become what are called strategic defaults; lawmakers strategically create defaults that force parties to reveal information about the contracting arrangement.[139] This is due to the fact that penalty defaults are drafted in a way to create an incentive for one party to contract around the default, thus disclosing their contracting position in the contract.[140] Therefore, if it is assumed that the party with the stronger bargaining power is the more informed party, defaults can force a more informed party to reveal more information to the less informed party.[141] Misinformed consumers enter bad deals,[142] and when misinformation is a growing concern in an industry, lawmakers can use default provisions to combat information imbalance. Furthermore, defaults may be so powerful in deterring information disclosure, that they become the governing term in the contract. A party, for fear of revealing information to the other party either about information relevant under the default provision or other aspects of the contract, may opt to claim the default penalty in the contract or fail to contract around it.[143] Therefore, lawmakers can create a default penalty that is favorable to the consumer that may make its way into the final contract.

---

138. *Id.* at 282.

139. *See* Ayres & Gertner, *supra* note 124, at 94 ("In particular, the possibility of strategic incompleteness leads us to suggest that efficiency-minded lawmakers should sometimes choose penalty defaults that induce knowledgeable parties to reveal information by contracting around the default penalty.").

140. *See id.* at 97.

141. *See id.* at 97–98.

142. *See* Shmuel I. Becher, *Behavioral Science and Consumer Standard Form Contracts*, 68 LA. L. REV. 117, 119 (2007).

143. *See* Ayres & Gertner, *supra* note 124, at 99–100 ("We suggest that a party who knows that a particular default rule is inefficient may choose not to negotiate to change it. The knowledgeable party may not wish to reveal her information in negotiations if the information would give a bargaining advantage to the other side.").

b. Consideration in Standard Form Contracts

Consideration is one of three fundamental elements of an enforceable contract: offer, assent, and consideration. Yet, this statement is deceiving as it treats consideration as an on-off switch. Courts certainly ask whether consideration is present in an arrangement or not, but "[i]nherent in that finding is a determination that the consideration has legal value."[144] The key word being "value," consideration can be better seen as a sliding scale: from no consideration, to the peppercorn,[145] up to a clear demonstration of consideration. However, the general rule is that courts will not question the adequacy of consideration, perhaps because it would be too difficult to police, and even if enforced certain forms of consideration would be hard to value.[146]

Courts have one exception to this general rule, unconscionability. When a court refuses to enforce a contract under the paternalistic contract doctrine of unconscionability, it does so assuming that parties did not understand the real interests that were the subject matter of the contract.[147] Unconscionability does not focus exclusively on gross inequality of bargaining power; however, such can be evidence of an unconscionable contract along with other facts, such as terms favoring the stronger party, deception, limited options for the weaker party, etc.[148] If unconscionability simply focused on bargaining power, corporations would face difficulty in contracting with consumers. Thus, the test is that unconscionability should be used to prevent "oppression and unfair surprise and not . . . disturbance of allocation of risks because of superior bargaining power."[149] But courts rarely use the doctrine, in part due to honoring the parties' agreements and in part due to the lack of definition of what truly constitutes an unconscionable contractual arrangement.[150]

Although the unconscionability doctrine of contracts may not play a large role in regulating contracts, the measurement of consideration is not wholly irrelevant. Consideration serves not only a role in contract formation, but a

144. Frank P. Darr, *Unconscionability and Price Fairness*, 30 HOUS. L. REV. 1819, 1827 (1994).

145. A peppercorn is consideration in name only. "A term often used in the past in expressing the consideration of a contract in which no more than a nominal consideration was intended." *Peppercorn*, BALLENTINE'S LAW DICTIONARY (3d ed. 1969).

146. *See* Darr, *supra* note 144, at 1825–26; *see also* Andrea M. Matwyshyn, *Privacy, the Hacker Way*, 87 S. CAL. L. REV. 1, 9 (2013). "[C]ontract law looks only for legal *sufficiency*, not adequacy, of consideration. Legal sufficiency inquiries for purposes of contract law merely look to whether the parties *subjectively value* the transferred things; courts generally prefer not to second-guess . . . ." *Id.* (footnote omitted).

147. *See* Darr, *supra* note 144, at 1825.

148. *See* RESTATEMENT (SECOND) OF CONTRACTS § 208 (AM. LAW INST. 1981).

149. Darr, *supra* note 144, at 1829 (quoting U.C.C. § 2-302 cmt. 1 (AM. LAW INST. & UNIF. LAW COMM'N 1990)).

150. *See id.* at 1830–31.

cautionary function in encouraging parties to evaluate the transaction.[151] This function is evident in the bargain test or bargain theory of consideration. The bargain theory of consideration is that reciprocation is not the main measure of whether there is consideration, but whether what was received was genuinely bargained for.[152] Even a peppercorn then can be sufficient consideration, however, this assumes that the party is well informed to appreciate the full details of the exchange. Although a peppercorn can be sufficient consideration for legal enforcement, does it still perform the cautionary function? It is unlikely. Studies suggest that consideration must be somewhat reciprocal, not nominal, to ensure that parties honor the contract.[153] This suggests that without some equality, or perceived equality, in the consideration, parties are more likely to breach the contract, likely because they do not fully appreciate that a contract was formed.

Issues of consideration are exacerbated when it comes to standard-form contracts, the most common form of contracting between companies and their customers. The bargain theory of consideration cannot be applied in its truest sense to standard-form contracts. If consideration is considered sufficient evidence that a contractual arrangement has been bargained for, thus serving as a proxy for a meeting of the minds, then if there is no meeting of the minds there can be no bargain, no consideration. Unless one considers a consumer's decision to take it or leave it with respect to a standard-form contract a meeting of the minds, under the bargain theory of consideration there can be no consideration.[154] But considering that most consumers do not even read the contracts that they are entering into, it seems even less likely that deciding to enter into a standard-form contract can constitute a meeting of the minds.[155] Contract law assumes that consumers know what they want and rationally

---

151. *See* David A. Hoffman & Zev J. Eigen, *Contract Consideration and Behavior*, 85 GEO. WASH. L. REV. 351, 353 (2017). Some scholars believe that consideration acts as a measure of the bargain which society believes is worth enforcing. *See id.* at 362.

152. *See Bargain Test of Consideration (Bargain Theory of Consideration)*, THE WOLTERS KLUWER BOUVIER LAW DICTIONARY (Desk ed. 2012).

153. A study was conducted to test a hypothesis on contract breach: whether a simple formality of recitation of consideration was sufficient to encourage parties to carry through a contract or whether more was required. Subjects were asked to distribute a donation of $2.00 between two charities. After the distribution amount was decided by the subject, the subject was tempted to back out of the bargain. The group that only saw a recitation of consideration was more likely to back out than the group that received a monetary consideration for $1.00 for the bargain. *See* Hoffman & Eigen, *supra* note 151, at 370–85. Because of the values used in the study, the results suggest "bonus effects in [the] study result from norms of reciprocity, rather than from the formality itself." *Id.* at 390.

154. Note that the question of whether a true meeting of the minds has occurred is a subjective intent question not an objective intent question. *See* Jordan M. Blanke, *"Robust Notice" and "Informed Consent:" The Keys to Successful Spyware Legislation*, 7 COLUM. SCI. & TECH. L. REV. 1, 33 (2006).

155. *See* Hoffman & Eigen, *supra* note 151, at 355–56. "[E]veryone has long acknowledged—and now we all know—that no one reads form contracts . . . ." *Id.* (footnotes omitted).

contract accordingly, but behavioral economics shows that this may not be the case.[156] Yet, standard-form contracts are indeed enforceable.

It seems then that at least for standard-form contracts, consideration's cautionary function may help to relieve this phantom consideration, where there is no true meeting of the minds. Perhaps if a cautionary measure is strong enough, it can be stated that the consumer did consider the terms and overall transaction and the bargaining did in fact take place. This theory would bring back to life historical formalities, such as the seal or notarization, which played a part in ensuring that parties to a contract appreciated the promises that were bargained.[157]

2. Notice and Consent as Applied to Online Contracts

In the modern technology era, online standard-form contracts have exacerbated the concerns that already plagued traditional standard-form contracts.[158] A clickwrap is where a consumer is shown terms and conditions for a licensing agreement and simply must click to consent to its terms,[159] regardless of whether the consumer has been confirmed to have read the terms. A simple clickwrap has enough formal consent for coordination for contract formation,[160] and as a general matter is an enforceable contract.[161] The quantity and speed of creation in these types of contracts is alarming in that they decrease the meaningfulness of consent.[162] Historically, meaningfulness of consent and contract formation was a function of formalities[163] such as seals. Seals increased compliance to promises made in a contract.[164] Consent did not need

156. *See* Becher, *supra* note 142, at 120 ("Given the cognitive limitations of ordinary people, consumers as a class frequently violate the rational-maximizing-expected-utility function that contract law theory ordinarily attributes to contracting parties. In other words, presuming the efficiency of form contract terms might be misguided due to fundamental behavioral failures on the part of consumers.").

157. *See* Hoffman & Eigen, *supra* note 151, at 35–54.

158. *See* Nathan B. Oman, *Reconsidering Contractual Consent: Why We Shouldn't Worry Too Much About Boilerplate and Other Puzzles*, 83 BROOK. L. REV. 215, 237 (2017) ("If anything, the advent of the computer and the Internet has decreased the costs of contracting, making boilerplate contracts even more ubiquitous.").

159. *See* Michelle Garcia, *Browsewrap: A Unique Solution to the Slippery Slope of the Clickwrap Conundrum*, 36 CAMPBELL L. REV. 31, 35 (2013).

160. *See* Oman, *supra* note 158, at 242.

161. *See* Garcia, *supra* note 159, at 43.

162. *See* Oman, *supra* note 158, at 240–41 (noting Margaret Radin's statement that an "[a]greement gets reduced to consent, then further reduced to assent. Next assent becomes 'blanket assent' to unknown terms, provided they are what a consumer—an abstract general construct of a 'consumer'—might have expected.") (quoting MARGARET JANE RADIN, BOILERPLATE: THE FINE PRINT, VANISHING RIGHTS, AND THE RULE OF LAW 82 (2013)).

163. *See* Hoffman & Eigen, *supra* note 151, at 356 ("But knowing if formalities retain their power online is important. We react to proposed contracts based on our interpretive models of what constitutes a legal 'contract.'").

164. *See id.* at 357.

to be strengthened in order to caution parties that their contracts came with legal weight. Although a bare seal has no legal meaning, parties who lacked expertise of contract law saw it as signifying a contract.[165] It created somewhat of a pause and realization effect. This is contrasted by clickwrap standard-form agreements, the purpose of which is to form quick contracts with ease.[166]

It is a generally known fact that consumers do not read contracts.[167] Even if the contract is read, there is question regarding if a consumer can process the cost and benefits; "the potential consumers of an intellectual product are often not in a position . . . to predict how valuable the product will be to them and how burdensome will be the limitation [of the terms] in question."[168] And yet, these contracts are rarely found to be unconscionable, even considering that most iconic cases on unconscionability involve standard-form contracts.[169] Thus, this sets the stage in introducing the dangers of relying on "self-management" by consumers in privacy law. Privacy self-management "provide[s] people with control over their personal data, and through this control people can decide for themselves how to weigh the costs and benefits of the collection, use, or disclosure of their information."[170]

Consent plays a large role in contract formation, it is essentially the assent element,[171] and in the economics of contract law, it solidifies the "meeting of the minds" concept in that both parties are acting with volition and information to benefit themselves; if there is no benefit, there is no contract.[172] Thus, consent acts as a coordination mechanism and, further, as a feedback mechanism: coordination showing that a bargain was formed and feedback in that there is understanding and a response to the contract in the form of an acceptance or denial.[173] Coordination is not the controversial issue; the feedback is.[174] When consent is shown to be voluntary and well-informed, only then can one draw conclusions from what the parties wanted.[175] Not all consent is meaningful.[176] Although it is true that there will always be a handful of consumers who read contracts and communicate any negatives out to the

165. *See* Hoffman & Eigen, *supra* note 151, at 365 ("[I]ndividuals believe that certain behavioral formalities—signatures and payment—create binding contracts, and they are not persuaded that contracts result merely from verbal or written language memorializing agreements.").

166. *See* Garcia, *supra* note 159, at 40.

167. *See* Hoffman & Eigen, *supra* note 151, at 387.

168. Garcia, *supra* note 159, at 62 (quoting William W. Fisher III, *Property and Contract on the Internet*, .73 CHI.-KENT. L. REV. 1203, 1245 (1997)).

169. *See* Oman, *supra* note 158, at 238.

170. Solove, *supra* note 76, at 1880.

171. *See* Blanke, *supra* note 154, at 28.

172. *See* Oman, *supra* note 158, at 216–17; Solove, *supra* note 76, at 1895.

173. *See* Oman, *supra* note 158, at 231–33.

174. *See id.* at 242–43.

175. *See id.* at 223.

176. *See id.* at 217.

general public, information sharing as a positive externality of few consumers' diligence, this is insufficient for certain types of contracts.[177]

Where the approach to regulation is self-management, the concern is how to ensure that consent is truly consent or what the consumer wanted. Simple recitals of consideration, or the bargain, do little to induce deliberation of parties to a contract.[178] They simply serve as an evidentiary function rather than a cautionary one. Therefore, there is a need for robust notice and meaningful consent to strengthen the cautionary function within contracts, especially when considering the speed at which consumers enter into clickwrap agreements. Robust notice, or "actual notice at the point of collection of the personally identifiable information describing briefly and succinctly the intent of the [collector] . . . to use or disclose that information for marketing or other purposes,"[179] notifies consumers of the legal ramifications of what they are agreeing to and informs them of the details.[180]

III. RESOLUTION

Delta's new facial recognition boarding process is just the beginning to what is an inevitable expansion of contractual transactions where companies provide services for access to consumers' faceprint. This expansion of FRT grows in an environment where there is no direct federal regulation and ineffective state regulation. Many of these companies bargain away small conveniences for a faceprint that can provide them with the key to access a hoard of information about consumers. And, as behavioral economics shows, consumers are quick to sign contracts without reading them, but if they were to read them, would they fully appreciate the contractual arrangement that they have bound themselves to? The lack of reciprocal consideration shows that it is unlikely. Thus, the two proposals for federal regulation focus on resolving two main issues: (1) consumers do not fully appreciate the value of the faceprint they are licensing to a company and thus default provisions are needed to inform consumers; (2) furthermore, the speed at which contracts are created in a world of standard-form contracts creates a need to develop a "super consent" model that forces consumers to respect the legal contract ramifications of faceprint licensing in which they are entering.

---

177. *See id.* at 247–48.

178. *See* Hoffman & Eigen, *supra* note 151, at 387–88.

179. Blanke, *supra* note 154, at 18 (quoting Online Personal Privacy Act, S. 2201, 107th Cong. § 401(13) (2002)).

> The only way a person can give truly informed consent is if he or she has received robust notice. This notice must include information sufficient to inform the person of the consequences of his or her action. Strict provisions for robust notice must be implemented in order to guarantee that an informed consent creates a genuine assent.

Id.

180. *See id.* at 13–14, 18.

A. The Problem in Context

When a consumer signs up for Delta's facial recognition boarding process, they are essentially licensing their faceprint in an exchange for the convenience of not having to pull out their boarding pass when boarding an airplane. If a consumer believes that the consideration exchanged is worth what he or she is giving up, there is no reason why paternalistic contract law should step in.[181] However, consumers do not seem to appreciate the value in the faceprint that they are licensing away.[182] This is because of cognitive and structural limitations that burden consumers.[183] Data and studies have shown that cognitively, consumers are unable to make informed, rational decisions when it comes to licensing their data or disclosing it.[184] Again, this is because few people read contracts, and few people opt-out. Generally, solutions have been proposed for more simple or visceral notice,[185] but both of these options simplify the complex nature of data disclosure and its ramifications.[186] Consumers simply lack the expertise to fully contemplate their actions.[187] This is why privacy law's self-management model and current laws' simplistic notice and consent models are not sufficient to protect consumers. Further, with the amount of data that is being disclosed to various entities, consumers are biologically unable to contemplate how this will affect them in scale and in the aggregate, considering the changes in contracts multiplied by the number of contracts across time.[188] For example consider PII, or "personally identifiable information," although some personal information that is considered PII is static, such as a social security number, PII can also be context-dependent;[189] PII could constitute the combination of an address and a birthdate, where neither alone are sufficient. Thus, consumers could consent their personal data piece by piece leading to an aggregation of information by other parties that could prove troubling ramifications for their privacy. This is why Senate Bill 847, with its increased information sharing, alone will not be sufficient to protect consumers.

The biggest strength of FRT-based authentication is that it cannot be compromised . . . yet. With spoof-protection,[190] hacking is made difficult, but

181. *See* Oman, *supra* note 158, at 222 ("Those with contractual capacity should be treated as adults entitled to make their own decisions.").

182. *See* Solove, *supra* note 76, at 1880–81.

183. *See id.*

184. *See id.*

185. *See id.* at 1885 ("'[V]isceral notice' may resuscitate the notice approach by attempting to make people experience notice more directly and emotionally.").

186. *See id.* at 1885.

187. *See id.* at 1887.

188. *See id.* at 1888–89 ("[T]he average person just does not have enough time or resources to manage all the entities that hold her data.").

189. *See id.* at 1891.

190. *See* Greenberg, *supra* note 53.

the technology is not perfect,[191] and if given the time, it is likely that someone will figure out how to take a stolen faceprint and hack into an FRT-based authentication system. Consumers are therefore licensing away the equivalent of a password, the value of which can be based on the information it is used to protect, on the premise that it cannot be stolen and used. But if it is stolen, there is no recourse. The ease of which consumers license their faceprint password away,[192] knowing most consumers do not read contracts,[193] is alarming and demonstrative of their naivete in the value of this data. Furthermore, companies can use FRT data to connect a consumer's online presence with his or her physical presence. Back in 2012, Target was able to deduce that a man's daughter was pregnant using its data mining system.[194] By linking a customer's credit card, name, and email address to a Target-generated guest ID number, it was able to collect data and analyze shopper's buying behaviors. If companies are able to close the gaps between our virtual selves and our "real world" actions, they would be able to better market their products. Thus, there is a sizeable value in FRT data, but consumers believe that they are giving up little to nothing.

> A common refrain in the privacy debate asserts that when consumers sign up for a "free" service, such as a Facebook account, they get what they pay for in terms of privacy—nothing. In other words, this argument alleges that consumers can demand nothing in terms of privacy and security from companies because the companies essentially gift their services to consumers: the consumer conveys no "thing of value" to the company.[195]

The idea that a consumer's faceprint is of little to no value is just simply untrue: for consumers it plays a huge role in authentication, and for companies it can be a valuable tool in further customizing target marketing.

B. Model Agreement and Default Provisions

The Uniform Commercial Code (UCC) governs sale of goods transactions, and its gap-filling function of providing default provisions provides efficiency in contracting, as well as protections. Thus, because of consumers' lack of appreciation and expertise for the consideration in FRT contracts, the industry would benefit from default provisions drawing out a model standard-form agreement. The model agreement would contain both default provisions and immutable provisions, saving the greatly paternalistic

---

191. *See* Korosec, *supra* note 53.

192. *See* Steele, *supra* note 8 (again noting that out of twenty-five thousand consumers of Delta's FRT boarding process, only two percent opted out of the service).

193. *See* Hoffman & Eigen, *supra* note 151, at 387.

194. *See* Kashmir Hill, *How Target Figured Out a Teen Girl Was Pregnant Before Her Father Did*, FORBES (Feb. 16, 2012, 11:02 AM), https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#2ac66b676668.

195. Matwyshyn, *supra* note 146, at 7–8 (footnote omitted).

immutable provisions for terms that would greatly mitigate data risk, such as a default number of years for data to be retained. Default provisions should be drafted against the company, the party with the stronger bargaining power, so as to force the company to fully reveal use of the data,[196] thus further showing the value in the data they are asking consumers to license to them; this forces a disclosure of especially useful information that a company has a private incentive to keep secret. Default provisions drafted in such a way are likely to result in a shift from the company to an increase in cost to the consumer; however, an increased cost to consumers may be beneficial to alert them to the legal ramifications of the transaction they are entering in.

C. Requirement of "Super-Consent"

The requirement of a "super-consent" model requires that consumers pause and appreciate the terms of the document. It requires meaningful consent in an era of fast contracting. The limitations of consumers are clear that even if they were to read contracts, they cannot process and make appropriate choices that would adequately protect their faceprint licensing. This leads to the assumption that without reading they have no chance in self-management of their privacy interests. Unfortunately, the lack of studies on consumer behavior and contract formalities makes it difficult to pinpoint an exact solution of what an effective "super-consent" model would look like.[197] And there will never be a fool-proof method of ensuring that consumers are reading contracts, but by increasing transaction costs of entering contracts, such as initialing of every clause or something symbolic such as the seal, consumers will be forced to slow down and reconsider the actions they are taking. Perhaps, some form of monetary consideration for notarization would serve a more cautionary function.[198] Unlike forcing an uneducated consumer to estimate the value of their faceprint license, complicated by the terms of use allowed and additional legal jargon, money has an easy-to-ascertain value.

D. Why Both

"[I]f Internet users read each of the privacy policies they encountered, they would each spend twenty-five days reading privacy policies every year, amounting to a nationalized number of 53.8 billion hours spent reading (unnegotiable) privacy policies."[199] Thus, emphasizing the need for both a model agreement for the FRT private commercial industry as well as a super-consent model. Knowing that consumers are unlikely to read a contract, and

196. *See* Ayres & Gertnert, *supra* note 124, at 107 ("Lawmakers therefore should not impose penalty defaults that have a net effect of reducing the amount of socially useful information.").

197. *See* Hoffman & Eigen, *supra* note 151, at 364 (stating that their study was the first of its kind on contract recitals). In addition, there was little found elsewhere on any specific studies that would be relevant.

198. *See id.* (showing that some form of easy to value reciprocal consideration can have a cautionary effect that forces parties to respect promises made in a contract).

199. Matwyshyn, *supra* note 146, at 2 (emphasis omitted).

less likely to read a long contract,[200] a model agreement would act as a gap-filler for the consumer-protective provisions and only those provisions that the company desires to contract around will be present in the actual agreement presented to consumer. This would decrease the language and increase the strength of the penalty default's information-generating function. A model agreement alone would function just as any clickwrap or online contract; thus, the super-consent model is needed. Without a model agreement, contracts would be lengthy and discourage consumers from reading the language. Thus, both are needed to have the full effect of changing the contracting process and terms.

CONCLUSION

In an age when technology is constantly advancing, it is not surprising that the general public has felt that they have lost control of their privacy.[201] "[I]nnovation depends upon privacy, which is increasingly under threat . . . ."[202] People are more willing to license away their data, including biometric data, when they seem to have more control, even if that control is illusory.[203] This consumer concern seems ironic when it is a generally known fact that consumers do not read the contracts that they enter in.[204] With the growing commercialization of biometric authentication technology, especially of FRTs and the unique dangers they possess, this quick and dirty contracting will not protect consumers when unregulated and only protected by the self-management system of privacy law protection.[205]

Consumers simply are not experienced, nor educated, enough to make determinations on licensing away their faceprint. Even if a consumer were to educate himself or herself on each contract signed, "[p]rivacy costs and benefits . . . are more appropriately assessed cumulatively and holistically."[206] Yet, no consumer is able to aggregate all of the contracts in which they sign away individual uses of their faceprint and assess how a little sacrifice here and there will affect their overall privacy. Currently, contract law barely plays any role in privacy law, mainly because privacy policies are not deemed to be

200. *See* Cakebread, *supra* note 116.

201. *See* Matwyshyn, *supra* note 146, at 2 ("Though clearly exaggerated for comic effect, the plot of this *South Park* episode correctly captures the feelings of many users: they have lost control of their privacy.").

202. Solove, *supra* note 76, at 1881.

203. *See id.* at 1887 ("Social science also reveals that privacy preferences are not developed in the abstract but in context. The way choices are framed, and many other factors, shape — and tend to skew — privacy preferences. People are also more willing to share personal data when they feel in control, regardless of whether that control is real or illusory.") (footnote omitted).

204. *See* Hoffman & Eigen, *supra* note 151, at 387.

205. *See id.* at 367 (noting that generally consumers are found to bear the blame, especially in form contracts, for poor contracting outcomes).

206. Solove, *supra* note 76, at 1881.

contractual in nature and because plaintiffs cannot show actual harm.[207] However, recent laws and judicial decisions have shown that technical violations are sufficient to prove harm[208] and thus, contract law can become relevant and powerful in privacy protection. "[C]ontract law is the lynchpin bridging consumer privacy promises in privacy policies with information security promises that arise partially out of terms and conditions of use. . . . [C]ontract law should . . . be embraced as a means of protecting consumer privacy more aggressively."[209] Contract law would allow regulations to move away from a paternalistic limitation of consent, but still protect consumer interests better than the current privacy law self-management model.[210]

A regulatory model, such as the one proposed here, encourages companies to communicate the value they receive when consumers license their faceprint and one that simultaneously forces consumers to appreciate the value that is given up will serve to caution consumers to re-evaluate what they are giving up and what little value they are truly receiving. Without an external source to serve this cautionary function, given the largely uneven bargaining power and largely uneven consideration, it is unlikely that the traditional elements of offer, consent, and consideration will be able to effectively protect users from the legal effect of their actions. In an age of multitudes of quick contract formations and fast technology advancements, consumers are susceptible to the dangers in licensing away an unreconcilable authentication key and naïve to what companies are doing with that data. Manageable information exchange, caution, and meaningful consent are the keys to protecting consumers from their own decisions.

207. *See* Solove & Hartzog, *supra* note 75, at 596–97.

208. *See* Rosenbach v. Six Flags Entm't Corp., 129 N.E.3d 1197 (Ill. 2019); *In re* Facebook Biometric Privacy Info. Privacy Litig., 185 F. Supp. 3d 1155 (N.D. Cal. 2016).

209. Matwyshyn, *supra* note 146, at 5 (footnotes omitted).

210. *See* Solove, *supra* note 76, at 1882 (stating that there is a complicated give and take if self-management were to cease to be the privacy law protection staple where consumers would have to be subjected to government paternalism, confining the freedom to contract).