Journal of Technology Law & Policy

Volume 25 Number 1

ARTICLES

DIGITAL GREENBACKS A SEQUENCED 'TREASURY DIRECT' AND 'FED WALLET' PLAN FOR THE DEMOCRATIC DIGITAL DOLLAR *Robert Hockett* 1

DEFENDING FACE-RECOGNITION TECHNOLOGY (AND DEFENDING AGAINST IT) *Henry H. Perritt, Jr.* 41

SURVEILLANCE CAPITALISM *William Hamilton* 141

Journal of Technology Law & Policy

Volume 25 Fall 2020 Number 1

DIGITAL GREENBACKS
A SEQUENCED 'TREASURY DIRECT' AND 'FED WALLET' PLAN FOR THE DEMOCRATIC DIGITAL DOLLAR

Robert Hockett[*]

Abstract

I propose means of immediately converting the Department of Treasury's existing Treasury Direct system of freely available transaction accounts into a publicly administered digital savings and payments platform. A platform of this type is an essential public utility in any commercial society such as our own. It is additionally growth-promoting inasmuch as growth-tracking Gross Domestic Product (GDP) is a measure of transaction volume, while transaction volume is a function of more efficient and inclusive transacting. As Congress seeks means of streamlining the payments infrastructure in a time of pandemic-induced crisis, the Treasury route recommends itself as the fastest way to digitize payments for 95% of our citizens and business enterprises. I also map means of migrating the Treasury architecture to the Federal Reserve System (Fed) over time once the crisis is past—as the "Greenback" paper dollar itself did in the late 19th and early 20th centuries—and include my draft Treasury Dollar Act as an Appendix.

INTRODUCTION 3

I. BACKGROUND: THE DEMOCRATIC DIGITAL DOLLAR, THE INCLUSIVE VALUE LEDGER, AND THE FED & TREASURY RENDITIONS THEREOF 5
A. *The IVL "Chassis"* 5
1. Basic Architecture 6
2. Pictographic Representation (Figure 1) 7
B. *Virtues of the IVL Chassis* 8
1. Justice and Inclusion 8
2. Growth and Efficiency 8
3. Fiscal and Monetary Policy (Including "Helicopter Money") Transmission 8

---

* Edward Cornell Professor of Law, Cornell Law School; Visiting Professor of Finance (Spring 2020), Georgetown McDonough School Of Business; Senior Counsel, Westwood Capital LLC; Advisory Board, Stanford Digital Currency Lab; Founding Board Member, Digital Fiat Currency Institute; Advisory Board, Public Banking Institute; formerly Federal Reserve Bank of New York and International Monetary Fund. Great thanks to New York Assemblyman Ron Kim; New York State Senator Julia Salazar; my Stanford colleagues Anshul Gupta and Lawrence Rufrano; my Commonwealth--associated colleagues Timothy Flacke, Howell Jackson, and Nick Maynard; and my Digital Dollar Project colleagues Chris and Charlie Giancarlo, who have been unremittingly brilliant, serious-minded, and encouraging. Needless to say, they do not all agree with all details that I set forth here.

4. Valuing Care Work 9
5. Data and Financial Privacy 10
C. *Federal Bodies for the Chassis—Fed or Treasury?*.....10
1. Why Federal? 11
2. Why Treasury? 12
3. Why—and When—the Fed? 13

II. THE TREASURY DIGITAL DOLLAR AND TREASURY DIRECT PLAN.....14
A. *Digitizing Treasury Direct* 14
B. *Functional Requirements* 15
1. Digitize Treasury Direct Accounts.....15
2. Make TDBs Legal Tender.....17
3. Add Horizontal P2P Connectivity.....17
4. Build-In Cryptographic Privacy Protection 18
5. Later, Consider Adding Interest on Accounts or Migrate to Fed and Do Same 18
C. *Technical Requirements* 19
1. The Accounts Layer 19
2. The Payment Layer 19
3. The Application Programming Interface Layer 20
4. It's Not That Difficult 20
D. *Pictographic Representation (Figure 2)* 21

III. THE DIGITAL FED DOLLAR AND FED WALLET PLAN.....22
A. *Why We Might Migrate* 23
B. *How We Might Migrate*.....26
1. Functional Requirements 26
2. Technical Requirements.....28
C. *Pictographic Summation & Synthesis* 29

CONCLUSION.....33

APPENDIX: THE TREASURY DOLLAR ACT OF 2020 34

INTRODUCTION

Since Facebook's announcement of its Libra proposal in June of 2019, monetary authorities worldwide have redoubled their efforts to develop central bank digital currencies (CBDCs).[1] These efforts were underway even before Libra, and for very good reasons. Facebook's announcement accordingly did no more than accelerate already ongoing developments.[2]

The sudden slowdown in productive activity worldwide brought on by the Coronavirus pandemic of 2020 makes matters more urgent. The social distancing measures necessitated by the pandemic are antithetical to productive activity—and, in turn, the *pay* people earn through productive activity.[3] "Knowledge workers" might be able to collaborate remotely, but production line workers and delivery personnel cannot.[4] Economies worldwide are thus confronted by simultaneous supply side and demand side shocks.[5] The U.S. economy is no exception—indeed it appears to be worst hit of all.[6]

---

1. *See* Robert Hockett, *Facebook's Proposed Crypto-Currency—More Pisces than Libra for Now*, FORBES (June 20, 2019, 2:03 PM), https://www.forbes.com/sites/rhockett/2019/06/20/facebooks-proposed-crypto-currency-more-pisces-than-libra-for-now/ [https://perma.cc/K9X8-8GFU] (explaining that the world's central banks are looking to upgrade their domestic and overseas payment systems by availing themselves of new technology).

2. *Id.*

3. *See* Robert Hockett, *An Immediate Relief Plan for Coronavirus-Related Economic Mitigation* 4 (Cornell L. Sch., Research Paper No. 20-28, 2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3567855 [https://perma.cc/5UPH-2THB]; Robert Hockett, *Managing Coronavirus's Economic Fallout—Demand and Supply Side Measures*, FORBES (Mar. 16, 2020, 1:02 PM), https://www.forbes.com/sites/rhockett/2020/03/16/managing-coronaviruss-economic-fallout-demand-and-supply-side-measures/ [https://perma.cc/P9PZ-PRKJ]; *see also* Robert Hockett, *We're at War and Need Wartime Institutions to Keep Our Economy Producing What's Necessary*, THE HILL (Apr. 4, 2020, 2:00 PM), https://thehill.com/opinion/white-house/491166-were-at-war-and-need-wartime-institutions-to-keep-our-economy-producing [https://perma.cc/KC57-TK4H] ('The virus . . . is threatening our way of life and destroying our productive capacity and economic health.').

4. *See* Robert Hockett, *White Paper: How to Mobilize the Military to Produce Pandemic-Responsive Supplies in Adequate Quantity*, NEW CONSENSUS 4 (Mar. 17, 2020), https://newconsensus.com/files/pandemic-production.pdf; Robert Hockett, *Our Corona Response's Missing Ingredient—Mobilize the Supply Side!*, FORBES (Mar. 18, 2020, 12:29 PM), https://www.forbes.com/sites/rhockett/2020/03/18/our-corona-responses-missing-ingredient--mobilize-the-supply-side [https://perma.cc/M7HJ-G36J]; *see also* Robert Hockett, *The US Must Take Equity Stakes in the Companies it Rescues*, FIN. TIMES (Mar. 28, 2020), https://www.ft.com/content/86a333d0-6dc3-11ea-89df-41bea055720b [https://perma.cc/LS99-6DDA]; Robert Hockett, *The US Needs to Tackle the Coronavirus Pandemic with a Playbook out of the Great Depression and World War II, not the Financial Crisis*, BUS. INSIDER (Mar. 29, 2020, 9:42 AM), https://www.businessinsider.com/coronavirus-pandemic-us-should-ramp-up-ventilator-mask-manufacturing-2020-3 [https://perma.cc/AM7S-FW89].

5. *See* sources cited *supra* notes 3–4.

6. *See* sources cited *supra* notes 3–4.

To arrest, minimize, and reverse these shocks, simultaneous demand and supply side measures must be taken as quickly as possible. This means that our capacities to store and transfer value—to make and receive payments and disburse moneys—must be sped up as well.[7] Whatever we are *able* to do, both to optimize our payments architecture and to speed up that optimization effort, we *must* do. In so doing, we will not only optimize a pandemic response architecture but also optimize the payments infrastructure, with which we shall live and prosper long after the present pandemic is past.[8]

Digital currencies are ideal means to this optimization. The reasons are straightforward. A currency is simply "that which pays" in a payment system and "that which counts" in a value accounting system.[9] To design a digital currency is to design a digital savings and payments platform. It is to design a literal speed-of-light mechanism of value storage and transfer. It is to deliver a banking and financial architecture by supplying a commercial architecture, as is the case in any "commercial society" or "exchange economy" such as our own.[10]

Fortunately, Congress is keen on this idea. Since late March, both Democrats and Republicans in both chambers have weighed proposals—including one of my own to which this Article is devoted—to pass legislation on a digital dollar and associated system of digital wallets. My own Inclusive Value Ledger (IVL) Plan, which has colloquially come to be known as the Public Venmo Plan since its draft bill was proposed in the New York State Assembly and Senate last year, can be instituted by municipal, state, or national authorities, and can be administered by either the Fed or Treasury at the national level.[11]

---

7. *See* Robert Hockett & Lawrence Rufrano, *Digital Dollars for All*, WALL ST. J. (Apr. 6, 2020, 7:18 PM), https://www.wsj.com/articles/digital-dollars-for-all-11586215100 [https://perma.cc/8TR9-BTDS]; *see also* Robert Hockett, *Why Now for a Digital Treasury Dollar? Because Coronavirus*, FORBES (Mar. 29, 2020, 8:36 AM), https://www.forbes.com/sites/rhockett/2020/03/29/why-now-for-a-digital-treasury-dollar-because-coronavirus/ [https://perma.cc/EE7Y-643V].

8. *See* sources cited *supra* note 7; *see also* Robert Hockett, Anshul Gupta & Lawrence Rufrano, *A Digital Dollar – Why, How, and Why Now*, VENTUREBEAT (Apr. 18, 2020, 12:12 PM), https://venturebeat.com/2020/04/18/a-digital-dollar-why-how-and-why-now/ [https://perma.cc/9JYZ-SHBJ].

9. Robert Hockett, *The Democratic Digital Dollar: A Digital Savings and Payments Platform for Inclusive State, Local, and National Money and Banking Systems*, 10 HARVARD BUS. L. REV. ONLINE, 2019–2020, at 1, 2.

10. *Id.* at 4; s*ee also* Robert Hockett, *The Capital Commons: Digital Money and Citizens' Finance in a Productive Consumer Republic* (2018) (unpublished manuscript) (on file with author) [hereinafter Hockett, *Capital Commons*].

11. *See generally* Robert Hockett, *The Empire State Inclusive Value Ledger: A Peer-to-Peer Savings & Payments Platform for an All-Embracing and Dynamic State Economy* (Cornell L. Sch. Research Paper No. 19-39, 2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3470923 [https://perma.cc/FBE7-EKRB].

For reasons rooted in both the "need for speed" and the need for inclusion in the midst of a pandemic, I aim with this Article to lay out my IVL Plan in both its Treasury and Fed renditions. The Treasury already possesses the requisite infrastructure for expeditious implementation and, partly for this reason, both Senators and Representatives in both party caucuses and in both chambers of Congress have been considering the plan since last March. There accordingly seems to be a need for a full discussion on the Treasury and Fed plans, their relation to one another, and their prompting considerations—including the simplicity and speed with which these plans, in comparison to others, can be sequentially set up and operated. This Article supplies these discussions. Part I provides background. Part II maps the Treasury plan. Part III charts the Fed plan. Part IV concludes and looks forward, while the Appendix includes a bill I have drafted for quick introduction and passage in Congress.

I. BACKGROUND: THE DEMOCRATIC DIGITAL DOLLAR, THE INCLUSIVE VALUE LEDGER, AND THE FED & TREASURY RENDITIONS THEREOF

I will begin by first sketching the basic structure that I believe a maximally efficient digital payment platform and wallet system will require, along with my reasoning for the structure. I will borrow a metaphor from the automotive sector and call this structure the plan's "chassis," onto which any number of distinct "bodies" selected by any level of government can then be installed.

A. *The IVL "Chassis"*

As noted above, my "Public Venmo" IVL Plan is already under consideration in New York. In the autumn of 2019 two visionary New York state legislators—Assemblyman Ron Kim and State Senator Julia Salazar—proposed legislation I had drafted to institute what I call a "Democratic Digital Dollar" and its associated "Inclusive Value Ledger," or "Public Venmo" platform.[12] In New York, we call it 'The

12. *Id.*; Assembly: https://www.nysenate.gov/legislation/bills/2021/A3138; Senate: https://www.nysenate.gov/legislation/bills/2019/s6792 A.B. A088686, 2019-20 Gen. Assemb., Reg. Sess. (N.Y. 2020), https://assembly.state.ny.us/leg/?default_fld=&bn=A08686&Summary=Y&Actions=Y&Text=Y. For a sampling of this author's columns and op-eds on the plan, several co--authored with the legislators who have introduced it to the New York state legislature, see, e.g., Assemblyman Ron Kim & Robert Hockett, *Dynamic Inclusive Money for a Dynamic Inclusive Economy*, AM. PROSPECT (Oct. 17, 2019), https://prospect.org/economy/dynamic-inclusive-money-economy/ [https://perma.cc/GHZ3-KQPD] (explaining why the economy must allow money to flow in a way that is 'inclusive'); Robert Hockett & Ron Kim, *Our New Currency for New York*, N.Y. DAILY NEWS (Oct. 28, 2019, 2:31 PM), https://www.nydailynews.com/opinion/ny-oped-new-currency-for-new-yorks-poor-20191029-uevs4nbx7fdwtbrlzgerdos664-story.html (explaining how the IVL will put money back into New York's economy and create a more even distribution of funds); Robert Hockett, Ron Kim & Julia Salazar, *Our Money's Not Green Enough*, FORBES (Nov. 9, 2019, 8:48 AM), https://www.forbes.com/sites/rhockett/2019/

Empire State Inclusive Value Ledger Plan.'[13]

Although this innovative legislation was introduced at the state level, the IVL Plan design is meant to function as a sort of "chassis" onto which any number of "bodies" can be installed at the local, state, *or* federal levels—not to mention counterpart levels in the Eurozone and beyond.[14] At the federal level, it can be established and administered by either the Fed or the Treasury.

1. Basic Architecture

The plan's architecture is strikingly simple. It requires only two functional steps. First, every person and business receives a smartphone or smart-device-accessible digital wallet, with both (a) "vertical" connectivity to the public treasury and (b) "horizontal" (essentially P2P) connectivity to all other digital wallets.[15] All wallet holders are then able "vertically" to pay taxes, licensing fees, and other remittances, as well as receive tax refunds, program moneys, and other disbursements over the IVL. Additionally, all users can "horizontally" make real time payments to one another.[16]

11/12/our-moneys-not-green-enough/ [https://perma.cc/YKM2-F8A5] (describing how the IVL system will work); Helen Partz, *Authors of New York's P2P 'Public Venmo' Bill Hope for Greater Decentralization*, COIN TELEGRAPH (Jan. 10, 2020), https://cointelegraph.com/news/ authors-of-new-yorks-p2p-public-venmo-bill-hope-for-greater-decentralization [https://perma.cc/4WUZ-L6LY] (describing how 'new technologies' will be used for the IVL); *New York Digital Currency Proposed for P2P Payments*, LEDGER INSIGHTS (Jan. 2020), https://www.ledgerinsights.com/new-york-digital-currency-proposed-p2p-payments/ [https://perma.cc/59CZ-CA6N] (explaining how others are working to recreate economic 'architecture'); Jordan Heal, *New York Lawmakers Propose Statewide Cryptocurrency*, YAHOO! FINANCE (Jan. 9, 2020), https://finance.yahoo.com/ news/york-lawmakers-propose-statewide-cryptocurrency-100001080.html [https://perma.cc/ WGZ9-7FXH] (describing the IVL cryptocurrency); *New York Lawmakers Push for Public eBanking System*, PYMNTS.COM (Jan. 8, 2020), https://www.pymnts.com/news/digital-banking/2020/ny-lawmakers-push-for-public-ebanking-system/ [https://perma.cc/K2AX-8E59] (outlining the "push" for an online banking system in New York); Jordana Rosenfeld, *New York Is Proposing the Creation of a 'Public Venmo,'* VICE (Jan. 7, 2020, 8:00 AM), https://www.vice .com/en_us/article/pked9v/new-york-is-proposing-the-creation-of-a-public-venmo [https://perm a.cc/AW5E-VES7] (describing the IVL as a "public Venmo").

13. *See* sources cited *supra* note 12 and accompanying text. On naming, one might envisage a comparable Lone Star IVL for Texas, a Crescent City IVL for New Orleans, a Continental IVL for the U.S., and so on.

14. *See* Robert Hockett, *Open the Marriage to Save It: A Peer-to-Peer Savings & Payments Platform and Complementary Digital Euro Plan* (Cornell L. Sch. Research Paper No. 19-40, 2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3470934 [https://perma.cc/W8EC-TGXS].

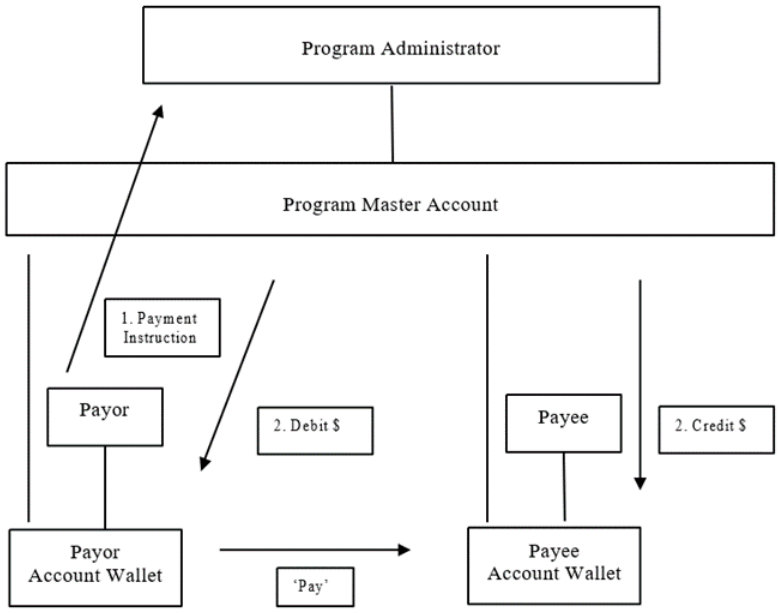
15. *See* Hockett, *supra* note 9; *see also* Hockett, *Capital Commons*, *supra* note 10; Robert Hockett, *Rousseauvian Money* 7 (Cornell L. Sch. Research Paper No. 18-48, 2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3278408 [https://perma.cc/W6DH-7CJT] (discussing vertical and horizontal dimensions).

16. *See* sources cited *supra* notes 9–12.

2. Pictographic Representation

Diagrammatically, then, things look as depicted in Figure 1.

Figure 1: Basic IVL Chassis



In the diagram, lines without arrows represent institutional linkages, while arrowed lines represent payment instructions and associated value flows. A payment occurs when the Payor instructs the Master Account Administrator, via a chip card, strip card, or smart device payment app (Payment Step 1), to debit her own wallet account in the Master Account and correspondingly credit the Payee's wallet account in the Master Account (Payment Step 2).[17]

At Implementation Stage 1 (the "vertical" stage) of IVL Plan implementation, counterparties in any such transaction will comprise one public and one private sector party. This is already possible through Treasury Direct Accounts as explained in Sections II.A.3 and III below.

17. I maintain a calculated ambiguity as among "wallets" and "accounts" throughout this Article for reasons rooted in fintech industry parlance. Pursuant to the latter, "wallets" hold "coins" that are legal tender, while "accounts" neither are nor "contain" legal tender, but instead represent liabilities on the part of account administrators to *tender* legal tender on account-holder demand. Where the issuer of the legal tender in question is also the administrator of the "account" in question, the distinction accordingly collapses—"wallet" and "account" then designate the same thing. See Hockett, *Capital Commons*, *supra* note 10, for full discussion.

At Implementation Stage 2 (the "horizontal" stage) of IVL Plan implementation, all wallet account holders in the system, public sector or private sector, will be able to make and receive payments to and from one another in the same manner. This is all that need be added to Treasury Direct wallets to convert them to universally functioning value-storage (saving) and value-transfer (payment) media.

B. *Virtues of the IVL Chassis*

There are a number of reasons, especially supplemented by recent crises-rooted needs, to put a proposal like the IVL Plan into place to get non-paper stimulus monies expeditiously to hard-hit American businesses and individuals.[18] We can briefly discuss those reasons here.

1. Justice and Inclusion

In any "exchange economy" such as our own, a payments system must be considered an essential public utility on a par with roads, sidewalks, and the national currency. Justice requires we make such utilities usable by all at no cost. Just as people do not pay to use sidewalks or dollar bills, they should not have to pay to use a digital payment system in an increasingly digitized exchange economy.[19]

2. Growth and Efficiency

We measure the size and the growth of our economy by reference to transaction volume.[20] That is all GDP is—a measure of transaction volume. It follows that a more seamless and efficient payment system, by enabling more rapid transacting and hence larger transaction volumes within any time interval, means greater growth and a larger economy over time. So does greater inclusion itself. Call this the growth or efficiency reason for IVL.

3. Fiscal and Monetary Policy (Including "Helicopter Money") Transmission

The presence of an IVL system, once in place, offers a host of collateral benefits. If administered by a nation's fiscal or monetary authority—the Treasury or the Federal Reserve in the U.S.—it will enable

---

18. Paper is a very efficient vector of Coronavirus, which is why China has been literally laundering its paper money since February. Jesse Yeung, *China is Disinfecting and Destroying Cash to Contain the Coronavirus*, CNN BUS. (Feb. 17, 2020), https://www.cnn.com/2020/02/17/asia/china-is-disinfecting-cash-coronavirus-intl-hnk-scli/index.html [https://perma.cc/H2JK-ZNUH].

19. *See* Hockett, *supra* note 9; Hockett, *Capital Commons*, *supra* note 10; Hockett, *Rousseauvian Money*, *supra* note 15.

20. *See* sources cited *supra* note 19; *see also* Kim & Hockett, *supra* note 12.

faster fiscal stimulus or monetary policy transmission than our present system of middlemen, whom we hope will transmit inexpensive credit to consumers.[21] Instead, we can drop digital "helicopter money" into our digital wallets, thereby sidestepping the notorious "pushing on a string" and diversion-to-speculative-use problems that hampered stimulus efforts in 2008.[22] In less extraordinary times, we can even offer interest on savings in wallets, whereupon we can move those rates up or down when we must slow down or speed up spending activity economy-wide.[23] Indeed, we can even then "micro-target" specific sectors of the economy where spending appears to be either overheating or dangerously cooling, another prospect considered below and more fully fleshed out in other work.[24]

4. Valuing Care Work

An IVL system would also enable public authorities, including cities and states, to begin disbursing monetary rewards to "care work" providers and other contributors to the public good that our present payment arrangements render too difficult for most governments to adjudge feasible.[25] A teenager who helps grade-schoolers with homework after school, for example, or someone who looks in on and cares for a "shut-in," can quickly transmit digital proof of work (POW) to a city, state, or even federal social services authority and receive spendable IVL credits—what I call Democratic Digital Dollars, or 3Ds—in return.[26] Given the long-term savings to municipal, state, and federal budgets that

---

21. *See, e.g.*, Hockett, *supra* note 9; Hockett, *Capital Commons*, *supra* note 10.

22. *See* sources cited *supra* notes 9–10; *see also* Daniel Alpert, Robert Hockett & Nouriel Roubini, *The Way Forward*, NEW AMERICA (Oct. 10, 2011), https://www.newamerica.org/economic-growth/policy-papers/the-way-forward/ [https://perma.cc/2ZZQ-744G].

23. *See* sources cited *supra* note 22. This is a prospect, incidentally, that might recommend—though certainly it does not mandate—migrating a Treasury system in time to the Fed, as discussed *infra* Section III.A.

24. *See, e.g.*, Robert Hockett, *How to Make QE More Helpful: By Fed Shorting of Commodities*, BENZINGA (Oct. 14, 2011, 8:41 PM), https://www.benzinga.com/news/11/10/1988109/how-to-make-qe-more-helpful-by-fed-shorting-of-commodities [https://perma.cc/6G87-DL32]; Robert Hockett, *The Green New Deal: How We Will Pay for It Isn't 'a Thing' – and Inflation Isn't Either*, FORBES (Jan. 16, 2019, 7:15 PM), https://www.forbes.com/sites/rhockett/2019/01/16/the-green-new-deal-how-we-will-pay-for-it-isnt-a-thing-and-inflation-isnt-either/ [https://perma.cc/7DZF-UTJV]; Robert Hockett, *Pay for the Green New Deal Now or Spend More Later*, FIN. TIMES (Feb. 3, 2019), https://www.ft.com/content/046e7c30-23c8-11e9-b20d-5376ca5216eb.

25. *See* Hockett, *supra* note 9; Hockett, *supra* note 11; Hockett & Kim, *supra* note 12, Kim & Hockett, *supra* note 12.

26. For examples of an IVL system's disbursing monetary rewards to 'care work' providers and other contributors to the public good, see sources cited *supra* note 25.

such work demonstrably affords, crediting over the IVL is readily justified on long-term fiscal grounds, let alone 'Good Society' grounds.[27]

5. Data and Financial Privacy

Finally, going digital offers financial data privacy benefits as well. Unlike private sector banks and many online payment service firms, public sector administrators of the IVL do not have a profit incentive—there are no non-criminal "carrots" to entice data harvest and sale. Such administrators also are subject to Fourth Amendment constraints as state actors. unlike, say, Wells Fargo or Facebook—there is a "stick." Adding *more* sticks through criminal law, moreover, along with especially hard encryption for all transactions in amounts lower than what we already require banks and other institutions to report under anti-terrorism and anti-money laundering law, is easily done on an IVL system.[28]

No matter how one looks at the matter, then, it seems clear we should do this. Commercial and financial inclusion, more rapid economic growth, leak-proof fiscal stimulus and monetary policy, valuing undervalued work, and tightening financial privacy . . . there seems little not to like. All such features, additionally, grow more attractive in times of crisis like the present.

The real question, then, is who best to administer the IVL. Should it be cities, states, or our federal government? If it's the latter, should it be the Fed or the Treasury?[29]

C. *Federal Bodies for the Chassis—Fed or Treasury?*

In light of the present pandemic and the nationwide financial stresses to which it is giving rise, it seems clear that whatever New York and other states or their subdivisions might do, we will do better to install a *federal* body on the IVL chassis than to rely solely on those more jurisdictionally circumscribed units of government.[30] The same reasons that underwrite this judgment seem to suggest also that the *Treasury* body would be preferable to the Fed body, at least in the short-run—even if we should decide ultimately to migrate the system over to the Fed, as we did with the paper dollar about a century ago.[31]

---

27. For support that crediting certain work over an IVL system is justified on long-term fiscal grounds in addition to "Good Society" grounds, see sources cited *supra* note 25.

28. For support that an IVL system can offer financial data privacy benefits, see sources cited *supra* note 25.

29. The Eurozone, of course, invites counterpart questions. Hockett, *supra* note 14, at 5.

30. *See* sources cited *supra* notes 1, 7–8.

31. Hockett et al., *supra* note 8. For more on that migration, along with the Greenback, see discussion *infra* Section II.A; *see also* Robert Hockett, *Money's Past and Fintech's Future: Wildcat Crypto, the Digital Dollar, and Citizen Central Banking*, 2 STAN. J. BLOCKCHAIN L. & POL'Y 221, 228–30 (2019).

1. Why Federal?

The reason that I designed the IVL plan to be adaptable to local, state, *and* national use in the first place, stems in part from lessons I learned in the last crisis. In 2008, at the onset of a *financial* meltdown rooted in an underwater *mortgage* loan meltdown, I developed a plan that permitted public sector entities to employ their eminent domain authority to make compulsory purchases of underwater mortgage loans out of the private label securitization (PLS) trusts in which they were improvidently locked, then write them down and return them to the trusts.[32]

These were loans that even trusts' bondholders wished to see written-down to avert default-prompted losses, as default risk lowered the expected values of mortgage loans by margins well below the level required to pull these loans back above water.[33] The problem was that neither scattered bondholders nor their PLS trustees could do the writing-down on an adequate scale.[34] For the pooling and servicing agreements (PSAs) pursuant to which PLS trusts had been settled, hastily drafted as they had been by lawyers who hadn't foreseen the prospect of a nationwide housing price crash and associated default wave, did not allow it.[35] If public authorities could partner with such bondholders to combine their own condemnation authority with bondholder money, I accordingly concluded, fair value condemnation awards could be paid at minimal or no public expense and the loans could at long last be written-down and thus salvaged.[36]

When it came to deciding what level of public authority to approach—state, federal, or municipal—I thought it best to try all. Hard-hit homeowners, cities, and states that could not wait for the Federal Housing Authority (FHA) or any other instrumentality to act to forestall foreclosures, evictions, and associated financial turmoil, even if federal action was, ideally, preferable.[37] In the end, then, while I started with federal officials and even Presidential candidates (then Senators Obama and McCain) in advocating the plan, it was ultimately hard-hit cities that

---

32. *See* Robert Hockett, *Paying Paul and Robbing No One: An Eminent Domain Solution for Underwater Mortgage Debt*, 19 CURRENT ISSUES ECON. & FIN., no. 5, 2013, at 1 (2013); Robert Hockett, *We Don't Follow, We Lead: How New York City Will Save Mortgage Loans Nationally by Condemning Them Locally*, 124 YALE LAW J. 131 (2014). In effect, the plan was meant to enable PLS trusts to do what commercial banks, which were not subject to PSA--rooted impediments, were already doing in voluntarily writing--down portfolio loans in NPV-- positive manners to salvage their expected values. The plan simply added a step to that process corresponding to the added entity—the PLS trust—interpolated between debtors and ultimate creditors.

33. *See* sources cited *supra* note 32.

34. *See* sources cited *supra* note 32.

35. *See* sources cited *supra* note 32.

36. *See* sources cited *supra* note 32.

37. *See* sources cited *supra* note 32.

acted once it became clear that the new Obama Administration was only going to pursue piecemeal "cram-down" in bankruptcy courts rather than plenary "write-down" in Congress or at FHA.[38]

In turning from the eminent domain plan to the IVL Plan several years after the mortgage loan crisis had finally receded, I kept the eminent domain plan experience in mind and accordingly started with our states and their cities at the same time that I approached federal officials and legislators, just in case. And while the *anticipated* case turned out to be *the* case for a time, with New York much quicker to act than was any other public authority,[39] the present pandemic appears to have changed things where speed and exigency are concerned. Now it seems that both Fed and Treasury, as well as both caucuses in both houses of Congress, might be ready to act.[40] The pandemic has denied us the luxury of waiting at *all* levels of government in our federal union.[41]

2. Why Treasury?

Now as already noted, the federal rendition of the IVL Plan is adaptable to both Fed and Treasury use. The latter would simply add two functionalities to Treasury's already existing network of Treasury Direct Accounts (TDAs), a long-standing but little known facility pursuant to which any citizen or legal resident of the US can already open a digital account through which to transact with Treasury in its own securities 24/7.[42] To convert this already existing platform into a universal digital

---

38. *See* sources cited *supra* note 32.

39. In this sense, contemporary New York might be likened to Governor Roosevelt's and State Industrial Commissioner Frances Perkins's New York, which pioneered many of the New Deal programs that Roosevelt and Perkins subsequently pushed as President and Secretary of Labor, respectively, of the United States. *See* Jessica Breitman, *Frances Perkins*, FRANKLIN D. ROOSEVELT PRESIDENTIAL LIBR. & MUSEUM, https://www.fdrlibrary.org/perkins [https://perma.cc/PW2D-Q69S] (last visited Oct. 16, 2020).

40. Philip Rosenstein, *COVID-19 Relief Could Be Catalyst for a Digital Dollar*, LAW360 (Mar. 26, 2020, 6:53 PM), https://www.law360.com/articles/1257079/covid-19-relief-could-be-catalyst-for-a-digital-dollar [https://perma.cc/TJQ2-URC7].

41. *Id.* The author of this Article is in discussions with Congressional staff on both sides of the aisle in both houses of Congress.

42. TREASURYDIRECT, https://www.treasurydirect.gov/ [https://perma.cc/BP46-ZXWE] (last visited Oct. 17, 2020). For recent writing done by the present author on TreasuryDirect and possible Treasury Dollars, see, e.g., Hockett, *supra* notes 7–8; *see also* Robert Hockett, *The Treasury Dollar: An Immediate Funding and Digital Banking Plan for Pandemic Relief and Beyond* (Cornell L. Sch. Research Paper No. 20-30), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3567829 [https://perma.cc/5AQY-PTS3]; Hockett, *How To Keep The Digital Dollar Democratic: A 'Treasury Dollar Bill' / 'Treasury Direct' Plan,* FORBES (Mar. 24, 2020, 2:35 PM), https://www.forbes.com/sites/rhockett/2020/03/24/how-to-keep-the-digital-dollar-democratic-a-treasury-dollar-bill--treasury-direct-plan [https://perma.cc/G8KC-TW92]; Robert Hockett, *The Democratic Digital Dollar: A 'Treasury Direct' Option*, JUST MONEY (Mar. 25, 2020), https://justmoney.org/r-hockett-the-democratic-digital-dollar-a-treasury-direct-option/

payment platform, we would need to take only two simple measures, which is why the draft bill appended to this article requires fewer than three pages of legislative text beyond Findings and Definitions.

The two steps, the first of which simply is Stage 2 of the IVL Plan schematized above in Section I.A.2 and Figure 1, are as follows: First, we add horizontal peer-to-peer (P2P) connectivity between TDA digital wallets to the current vertical connectivity between Treasury itself and all TDAs, as explained above in Section I.A.2. Second, we confer legal tender status on the Zero Percent Certificates of Indebtedness that Treasury already issues through TDAs—I call them Treasury Dollars, or Digital Greenbacks in honor of the national dollar that Treasury issued from the mid-1860s until the Fed's establishment fifty years later.[43] Even these two measures would be unnecessary if more than 75% of our population were banked because Treasury Direct already interfaces—indeed, at present *must* interface—with traditional bank accounts. But because 25% of Americans are unbanked or under-banked while only 5% lack smartphones or comparable devices, these two tweaks would be important.[44]

3. Why—and When—the Fed?

The other way to proceed—the alternative to building out Treasury Direct—would be to do something much like what I have just described but to do it through the Federal Reserve System instead, as elaborated below in Part IV.[45] In the long run, this might be preferable since the Fed conducts most of our monetary policy and we might wish to keep it that way.[46] In the short run, however, going the Fed route would be rather more difficult and, therefore, more time consuming—for the Fed, unlike

---

[https://perma.cc/DZ4E-EH8D]; Robert Hockett, *Money in Context: Part 2*, LPE PROJECT (Apr. 9, 2020), https://lpeproject.org/blog/money-in-context-part-2/ [https://perma.cc/78JM-JBPJ].

43. *See* sources cited *supra* note 42. The Greenback, incidentally, was virtually identical to the later Federal Reserve Note—same imagery and iconography, same size and material, etc. All that differed was the subtle inscription across the top, which of course did not read "Federal Reserve Note" until we migrated the Greenback over to the Fed after 1913. The Greenback history, incidentally, accounts for what might seem an idiosyncratic name that we continue to give to one of our primary bank regulators, the Office of the Comptroller of the Currency (OCC), so named because this office in Treasury actually *did* once control the currency. *See* Hockett, *supra* note 31.

44. *2017 FDIC National Survey of Unbanked and Underbanked Households*, FDIC 23, 34 (Oct. 2018), https://www.fdic.gov/householdsurvey/2017/2017report.pdf [https://perma.cc/8C5G-EEXS].

45. *See* discussion *infra* Part III; Hockett, *supra* note 9; Hockett, *Capital Commons*, *supra* note 10.

46. *See* Hockett, *supra* note 9, at 16; *see also* Hockett, *Capital Commons*, *supra* note 10. It is also possible that we will in the future elect to consolidate some Fed and Treasury functions that now occur separately. I discuss what consolidation might look like at length in *Capital Commons* in particular.

the Treasury, has no preexisting network of wallet-convertible individual and small business accounts.

My own view is that whatever we can do most quickly is what we should do now, with optimization to be addressed later.[47] And if I am right in my conjecture that this means beginning with Treasury and only later migrating to the Fed—again as our nation's first currency, the Treasury administered Greenback regime introduced in 1863, did in converting to the Federal Reserve Note regime 50 years later—then so be it.[48]

As just suggested, both for the reasons adduced immediately above and for additional reasons adduced below, I think the Treasury route is best for now, with migration to the Fed to come only later, if at all, once the pandemic is past and the Fed is reformed on the basis of lessons we're already learning.[49] To the details of both plans I accordingly now turn, starting with Treasury and then proceeding to the Fed.

II. THE TREASURY DIGITAL DOLLAR AND TREASURY DIRECT PLAN

Both for the reasons just noted and for additional reasons I lay out below, I think it best to debut the Digital Dollar as a Treasury Dollar or Digital Greenback, then migrate it over to the Fed, if at all, only after the present pandemic is past us. Here is how.

A. *Digitizing Treasury Direct*

Few seem aware of the fact, but the U.S. Treasury already affords any citizen or legal resident who desires it a TDA with the Treasury itself. Through this portal, citizens and legal residents can purchase or sell all four of the principal classes of Treasury security—bills, notes, bonds, and

47. *See* Hockett, *supra* note 7; Hockett, *supra* note 8; A.B. A088686, 2019-20 Gen. Assemb., Reg. Sess. (N.Y. 2020) (pending bill in the New York State Assembly for creating a master account and system of individual wallets to make and receive payments to state entities and residents of the state); *see also* Hockett, *supra* note 12 (discussing the proposed Inclusive Value Ledger which would enable the free flow of money during coronavirus); *Our New Currency for New York*, *supra* note 12 (discussing the benefits of the proposed Inclusive Value Ledger to New York residents); *Our Money's Not Green Enough*, *supra* note 12 (discussing how the Inclusive Value Ledger can dispose of the limitations on privately-run payment platforms); Partz, *supra* note 12 (giving a general overview of IVL and why it is being proposed); *New York Digital Currency Planned for P2P Payments*, *supra* note 12 (discussing the IVL proposal and the features of the ledger); Heal, *supra* note 12 (describing the features of the IVL and its purpose); *New York Lawmakers Push for Public eBanking System*, *supra* note 12 (describing the IVL as a solution to the millions of Americans who are excluded from the formal banking system); Rosenfeld, *supra* note 12 (describing IVL and distinguishing it from Facebook's Libra cyprocurrency).

48. Hockett, *supra* note 31, at 6.

49. *See generally* Robert Hockett, Spread the Fed: Distributed Central Banking in Pandemic and Beyond (May 10, 2020) (unpublished manuscript) (on file with author), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3597724 [https://perma.cc/T99G-WXT2].

TIPS—at any time, 24/7. All that is needed is: (a) an internet accessible laptop, smartphone, or other device; (b) a Social Security or Taxpayer ID number; and (c) a bank account out of which payments for, and into which redemptions of, Treasury securities can be made.

All that is needed to make this a full Treasury-administered Democratic Digital Dollar and IVL, then, is to add one new Treasury security endowed with legal tender status—a kind of digital cash—to the basket now offered and to establish horizontal connectivity between TDAs to supplement the vertical connectivity between these accounts and the Treasury by making them P2P-interactive.

Here, then, is the nucleus of what can be quickly scaled up into a national savings and payments platform administered by Treasury during the pandemic, then perhaps migrated over to the Fed when there is time to build out the Fed's digital infrastructure. I will begin with functional requirements, then turn to technical requirements.

B. *Functional Requirements*

Because Treasury Direct is already halfway there en route to a full digital dollar and payment platform, the functional adjustments requisite to conversion are simple and straightforward.

1. Digitize Treasury Direct Accounts

First, the Treasury will be explicitly authorized and indeed required to either: (a) allow digital dollars (digital Federal Reserve Notes) to be held in and spent from TDA Wallets, or (b) issue a new denomination of Treasury bill with no coupon or maturity date and a face value of $1. We'll call it a Treasury Dollar Bill (TDB) or Digital Greenback (DG). There is a sense in which Treasury already administers the seed of a TDB or DG: The Zero-Percent Certificate of Indebtedness (in Treasury shorthand, the "Zero-Percent C of I," or "C of I," and in my parlance "Zero-CI") is a Treasury security that does not earn any interest. It is intended, according to the Treasury, to be used as a source of funds for purchasing eligible interest-bearing Treasury securities in TDAs.[50] Treasury arguably already possesses authority to digitize Treasury Direct in this manner and even to issue a new legal tender Treasury Dollar. But "helicopter drops" into new starter accounts would require explicit Congressional appropriation, so we might as well explicitly authorize and indeed mandate the new issuance in the same initial appropriation legislation.

---

50. *TreasuryDirect Help: Zero-Percent Certificate of Indebtedness*, TREASURYDIRECT, https://www.treasurydirect.gov/indiv/help/TDHelp/help_ug_152-CofILearnMore.htm [https://perma.cc/9RXC-7V4K] (last visited Oct. 17, 2020).

The Treasury-Dollarized Zero-CI will effectively be a one-dollar perpetual, a.k.a. consol, much like the Federal Reserve notes we call dollar bills. Treasury will directly convey Congressionally determined amounts of these Treasury Dollar Bills, which I will call "Starter Deposits," to holders of TDAs, which can be digitized into digital wallets as described below. There will be no need, then, to 'sell' these Bills to convey them—a critical difference from other Treasury issuances. Starter Deposits, perhaps started with CARES Act style disbursements or "Baby Bonds" of the kind contemplated by sundry developed nations in the late 1990s and early 2000s, then can be periodically supplemented by what we will call Supplemental Deposits as Congress determines.[51] We can also cap digital TDB amounts held in TDA wallets, if we wish, as Treasury itself used to cap Zero-CIs. All else being equal, I would not myself favor such capping, but all else might not be quite equal.[52] Existing banks and payment companies might object to unlimited TBD amounts, for example, for fear of being rendered superfluous by a once again solely publicly issued payment medium. Financial stability imperatives might operate to similar effect—if, say, mass migration of deposits from private sector banks to digital TDA wallets would suddenly drain most of the banking sector's liquidity base.[53]

The latter danger could, of course, be well mitigated, if not eliminated, through Treasury lending to banks in the same dollar amounts as migrate from bank accounts to TDA wallets.[54] But that might take a while to work out, not to mention to work out to the satisfaction of frightened bankers. So, I suggest that we start TDA wallets simply with such future stimulus payments of the CARES Act variety as we make available for the remainder of the present pandemic, or with Baby Bonds as noted above.[55]

Treasury Direct wallet accounts holding TDBs will be much like accounts held with present-day money market mutual funds (MMFs), save that they will be sovereign issuances with all the guarantees thereof. TDBs will, for their part, be reminiscent, again, of the Greenback dollar bills that the Treasury issued as the nation's primary currency from the mid-1860s until early in the 20th century—when the Fed was established, and Fed Notes began to supplant Treasury issuances as primary currencies.[56] Hence my suggestion of Digital Greenbacks is an alternative name for TDBs.

---

51. *See* Robert Hockett, *A Republic of Owners*, YALE U. PRESS (forthcoming 2021) (discussing Baby Bonds as piecemeal asset-spreading policies). *See generally* Robert Hockett, *A Jeffersonian Republic by Hamiltonian Means*, 79 S. CAL. L. REV. 45 (2005); Coronavirus Aid, Relief, and Economic Security Act or CARES Act, S. 3548, 116th Cong. (2020).

52. See Hockett, *Capital Commons*, *supra* note 10, for more on when to cap and not to cap.

53. See *id.*, for full consideration of such prospects and means of mitigating them.

54. *Id.*

55. *See* sources cited *supra* note 51.

56. *See* Hockett, *supra* note 31.

2. Make TDBs Legal Tender

Second, if we do not mandate the permission of TDA Wallets to hold digital Federal Reserve Notes, then, through legislation, we will mandate either: (a) that henceforth Treasury Dollar Bills will be legal tender on the same footing as Fed dollar bills, or (b) that the Fed will open individual deposit-cum-transaction accounts—we will call them Fed Transaction Accounts (FTAs)—for all who have TDAs, with free transferability of funds between each pair of twinned Fed Transaction and TDAs.[57] Any and all such accounts will be digitized into smart-device-accessible digital wallets as we upgrade the national payments infrastructure as most developed nations are now planning to do.[58]

TDBs will thus constitute Congressionally determined helicopter money that functions alongside garden-variety Fed-administered money. Of course, the Treasury will coordinate with the Fed to prevent undesired inflationary impacts.[59] Because what occasions helicopter drops is essentially by definition a significant contraction, however, this seems unlikely to become an issue.[60]

3. Add Horizontal P2P Connectivity

Third, we supplement the currently open vertical connectivity channel between the Treasury and TDA wallet holders with universal P2P horizontal connectivity among all TDA wallet holders themselves.[61] We do that either between TDAs themselves, in the event that we opt for Option (a) just above, or between FTAs, in the event that we opt for Option (b) above. Again, then, TDAs or FTAs will become digital wallets, out of which anyone can pay anyone else for anything legally sold and into which anyone can be paid by anyone else for anything legally sold or conveyed.

As in my Democratic Digital Dollar and IVL plans more generally, private sector banking institutions can also be required, as a condition of licensure, to be among those businesses with what I call horizontal connectivity to TDA wallet holders. In that capacity, they can be required to offer full, fee-free access to teller windows, ATMs, and all other facilities at which anyone might wish to convert TDBs into Federal Reserve Notes (FRNs), coins, or any other form of legal tender cash we

---

57. For more on the prospect of Fed-administered digital dollars, see discussion *infra* Section II.C.4; Hockett, *supra* note 31; Hockett, *Capital Commons*, *supra* note 10. The latter work also discusses previous digital dollar and non-digital Fed account proposals proffered by various friends and colleagues of the authors since 2014.

58. *See infra* Section II.C.4; *see also* sources cited *supra* note 57.

59. See Hockett, *Capital Commons*, *supra* note 10, for a detailed design for Fed and Treasury coordination and even partial consolidation can be found in.

60. *Id.*

61. *See* sources cited *supra* note 19 and accompanying text.

might ever include among our money forms. But of course, this added feature can also be forgone if Congress fears backlash from bank lobbyists.

4. Build-In Cryptographic Privacy Protection

Fourth, we will cryptographically protect all TDAs or FTAs, and all transactions performed with them. We should also guarantee cash-reminiscent anonymity of transacting for all transactions in amounts not already required to be reported to bank regulators under current bank privacy and money laundering enforcement laws. Violations of these protections by any government official will not only constitute Fourth Amendment violations, but will also be legally prosecutable—as, of course, will be any breaches by hackers or other miscreants. Because the Treasury, unlike private sector banking institutions and payment service providers, is not actuated by a profit motive, security and data protection seem likely to be easier assured on the new Treasury Direct system than they are now. But there is no need to leave this to chance.

5. Later, Consider Adding Interest on Accounts or Migrate to Fed and Do Same

Finally, once the system is fully up and running, we might commence paying interest on funds held in TDAs or FTAs in the future, just as the Fed now pays interest on reserves (IOR) to banks holding accounts with it and as private sector banks pay (minimally) on checking and savings accounts held with them.[62] One reason for doing this is that it will afford our monetary authority—be that the Fed, Treasury, or a consolidated fiscal and monetary authority such as that I design in other work—a direct and hence very effective monetary policy tool. Rates can be raised immediately to slow spending, and can be lowered to boost spending, rather than changing them indirectly through bank rate policy.[63]

Should we go this route, in other words, there will be no more pushing on a string problems or other leakages in monetary policy transmission. Nor need we hope banks will lend or hope people will borrow in crises.[64] We will simply drop money in when we must, soak it back up other ways—raising rates higher, impounding some funds, or raising taxes if necessary.[65] As CPI inflation seems to have been lower than policy targets for decades now, though, that seems a fairly remote possibility.[66] We shall soon see whether productivity-drops owing to social distancing

---

62. See sources cited *supra* notes 9–10, 31 and accompanying text, for more on this prospect, why it might be considered attractive, and how it might be employed.

63. *See* sources cited *supra* note 62.

64. *See* sources cited *supra* note 62; *see also* Alpert, Hockett & Roubini, *supra* note 22.

65. *See* sources cited *supra* note 62.

66. *See* sources cited *supra* note 62.

during the pandemic will increase CPI inflation to meet or exceed policy targets.[67]

C. *Technical Requirements*

What, more specifically, does the technology look like for converting Treasury Direct Accounts into Treasury Dollar wallets for citizens, legal residents and businesses, without requiring them also to maintain separate private sector bank accounts? It is, believe it or not, not at all complicated. There are several key layers of any such system, and only one has yet to be built.

1. The Account Layer

First is the account layer. There must be safe, secure accounts that have reliable "know your client" (KYC) identity authentication protocols. These accounts are what function as users' virtual wallets, in which users can safely store, from which they can send, and into which they can receive digital dollars. They are essentially bank accounts with smart device keypads instead of brick-and-mortar storefronts. Critically, wallet holders have instant access to their funds, which is not the case with Venmo, PayPal, or other already existing private sector payment platforms that depend upon multi-day automated clearing house (ACH) operations to finalize payments. TDAs already possess most of these features, and can be readily upgraded within weeks or days, not months or years, to complete the replication.[68]

2. The Payment Layer

Second is the payment layer. There must be a real-time capacity allowing for simultaneous debiting of payor accounts, and crediting of payee accounts, if wallets are to outperform traditional bank or payment accounts along with the ease and speed of transacting dimension. The Federal Reserve, as is by now widely known, is developing such a system, "FedNow," for clearing between banks—a welcome development, but one whose completion (a) stands to benefit only banks and those holding bank accounts, and (b) for reasons unknown, is continuously postponed by the Fed.[69] Treasury can readily supply the same among all Treasury Direct wallets, and more quickly—the

67. See sources cited *supra* notes 3–4, for a discussion of pandemic-wrought supply side dangers.

68. A surprising multitude of this author's friends and colleagues in the tech sector, amusingly enough, use precisely the same phrase in this connection—a "piece of cake." Special thanks, incidentally, to Anshul Gupta, with whom I have worked for a long time indeed in getting the tech design right.

69. *See* FedNow Service, FED. RSRV., https://www.frbservices.org/financial-services/fednow/index.html [https://perma.cc/LG8U-45KW] (last visited Oct. 16, 2020).

technology, again, has long been familiar in the financial technology industry.[70]

3. The Application Programming Interface Layer

Third is the application programming interface (API) layer. This enables interoperability between the system being developed on the one hand, and various verified 3rd-party services, including PayPal, Venmo, merchant POS systems, and cross border payment services on the other hand. These integrations will be desirable insofar as there continue to be other ways to send money to friends, family, and businesses—which we might well desire for purposes of at least some resilience-assuring redundancy in the payments system. But it is worth also bearing in mind that the upgraded Treasury Direct system is meant to enable costless payments among all parties who pay or are paid in legally permissible transactions, such that any other systems out there are strictly speaking unnecessary, even if desirable for some purposes.

4. The Ledger Layer

The final layer is that of the ledger—in this case, the Treasury Direct accounting system as a whole, as administered by the Treasury. There must be a transaction-aggregation locus and a node through which to inject Treasury Dollars into the money supply for purposes of recipient self-maintenance and macroeconomic stimulus. The ledger can be distributed and thus grounded in blockchain technology, or can be centralized, as Treasury Direct is now. If we ultimately decide to go the former route, then we might see some increased complexity in implementation as we make architectural decisions concerning encoding keys, hashing, and hot/cold storage. Yet the underlying functionalities and requirements do not change, and in any event, we can convert Treasury Direct as currently constituted to P2P use without having to wait. Then any subsequent move to a blockchain or other distributed ledger technology (DLT) can be planned and executed at our leisure.

5. It's Not That Difficult

The technology involved in a Treasury Direct upgrade is, then, not trivial to build, but neither is it daunting or especially challenging. The requisite conversion involves technology with which both the industry and other agencies of our deferral government are well familiar. Indeed, the latter already has departments whose personnel are charged precisely with performing the very tasks just elaborated. One is the United States Digital Service (USDS), which is housed in the Executive branch of our

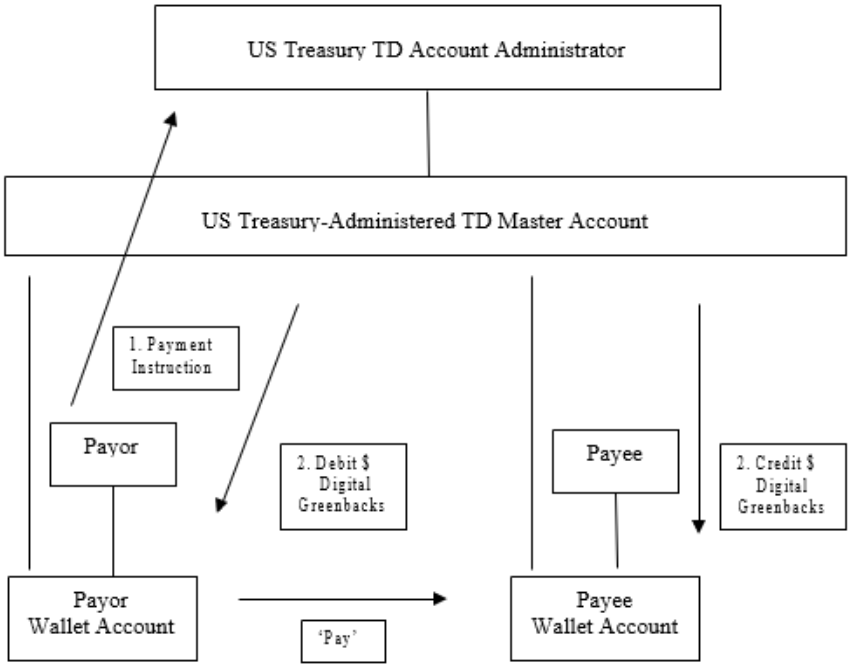
70. *Supra* note 68.

federal government.[71] Others are—unsurprisingly when you think about it—the Internal Revenue Service, itself housed in Treasury, and the Social Security Administration. While we might (or might not) wish to consult with private sector experts, then, in tweaking the Treasury Direct system into a network of digital wallets, it is noteworthy that we need not.

D. *Pictographic Representation*

In any event, the upshot once we are through will look as depicted in Figure 2, which the reader will note is isomorphic to Figure 1 above.

Figure 2: U.S. Treasury-Administered TDA Payments System



In the diagram, non-arrowed lines again represent institutional linkages and arrowed lines represent payment instructions and associated flows. A payment occurs when the Payor instructs the TDA Account Administrator, via a chip card, strip card, or smart device payment app (Payment Step 1), to debit her own wallet account in the TDA Master

71. *See* US DIGIT. SERV., https://www.usds.gov/ (last visited Oct. 16, 2020).

Account and correspondingly credit the Payee's wallet account in the TDA Master Account (Payment Step 2).

At Implementation, Stage 1 of Plan Implementation, counterparties in any such transaction will comprise the Treasury and one private sector party—that is effectively what is possible through Treasury Direct Accounts now, albeit not yet in Treasury Dollars or Digital Greenbacks, which I am proposing to institute. At Implementation Stage 2 of Plan Implementation, all wallet account holders in the system, public or private, will be able to make and receive payments to and from one another in the same manner. This is all that need be added to Treasury Direct wallets now to convert them to universally usable value storage (savings) and transfer (payment) media.

III. THE DIGITAL FED DOLLAR AND FED WALLET PLAN

While Treasury Direct seems the obvious route to go in digitizing the dollar in the short run, we might nevertheless wish to migrate any national rendition of the IVL system over to the Fed in the long run. The primary reason for doing so would be to keep the digital dollar fully integrated, under one administrator, with the nation's broader monetary policy apparatus and payments system—both of which are presently conducted and administered respectively by the Fed.[72]

This need, not to mention objections from the banking sector, might be less pronounced if TDA wallets were limited to low threshold ceiling amounts, but would grow if those ceilings were raised or eliminated. Similarly, if the Treasury Direct system is only sporadically used—for example, only for occasional and infrequent helicopter drops during a crisis—it also could presumably stay within Treasury, which could simply make certain to coordinate closely with the Fed during these ad hoc intervals as it always does in such circumstances.[73] This should in theory present no more difficulty than does the fact that there already are many bank deposit substitutes that the Fed must monitor even while not directly controlling them.[74]

If, on the other hand, we wish to maintain an ongoing digital dollar system making use of wallets free of any ceilings, then there will be at least some reason, even if not necessarily a dispositive reason, to migrate it over to the Fed—again rather as we did when we gradually replaced the Treasury Greenback regime, our first ever and principal paper currency system from the late- mid- 19th century to the early 20th century,

72. See Hockett, *supra* note 9; Hockett, *supra* note 31; Hockett, *Capital Commons*, *supra* note 10, for full discussion of present arrangements, why we have them, and why if at all we might wish to alter them.

73. *See* sources cited *supra* note 72.

74. *See* sources cited *supra* note 72.

with the virtually identical Federal Reserve Note after 1913.[75] The dollar system as now constituted represents a portion of the liability side of the Fed balance sheet—hence the term "Note," which abbreviates "Promissory Note," which we find atop all dollar bills.[76] And to these liabilities correspond assets.[77]

In theory, the Treasury could borrow from account holders willing to credit the Treasury through their TD Wallet Accounts just as the Fed in accounting terms borrows from dollar holders. It could even pay a coupon on such credits—in effect, interest on digital dollar deposits—in a manner that renders them functionally equivalent to both (a) Fed Reserve Accounts that now pay out Interest on Reserves (IOR) to banking institutions, and (b) Treasury Notes, Bills, and Bonds that pay out a premium to investors.[78] This would carry the Treasury well into the realm of central bank monetary operations, however, the full ramifications of which exceed the scope of interest of this Article though not of other work done by the author.[79]

The reader is accordingly asked simply to bear in mind that the functionalities of the Fed rendition of the IVL Plan—let's call it a FedWallets plan—that I shall now sketch all could *in theory* be discharged by the Treasury or a single consolidated authority performing all of the functions now separately distributed over our fiscal and monetary authorities, but in practice would then require we make basic structural changes to Treasury practice and associated accounting.[80]

If one day the U.S. should decide that central bank independence has been oversold and should be diminished or parted with, some such consolidation of funding, money-modulating, and liability-issuing authority might well be affected as it was in other eras of our nation's financial history.[81] For the present, however, the plan-sketching proceeds on the assumption that the nation retains separate fiscal and monetary authorities—that is, a separate Treasury and Fed.

A. *Why We Might Migrate*

A FedWallet rendition of the IVL Plan could either replicate the Treasury rendition and administer it as a separate functionality in parallel with the Fed's other functionalities or could integrate the Treasury into a more ambitious programmatic. The latter option would employ the IVL Plan not only as a national payments platform, associated Democratic

75. *See* sources cited *supra* note 72.
76. *See* sources cited *supra* note 72.
77. *See* sources cited *supra* note 72.
78. *See* sources cited *supra* note 72.
79. *See* sources cited *supra* note 72.
80. *See* sources cited *supra* note 72.
81. *See* sources cited *supra* note 72.

Digital Dollar, and public option for traditional retail banking—that is, value storage and transfer as outlined above—but also as an architecture for a far more effective channel of monetary policy and even more national investment than we have now.[82]

In the case of monetary policy, which central banks and monetary authorities traditionally conduct with a view to maintaining balance between money aggregates and productive potential, the Fed transacts with publicly favored "dealer banks" and other privileged financial institutions to effect policy.[83] It (a) buys or sells Treasury securities in such transactions to grow or shrink monetary aggregates, (b) changes interbank lending charges to affect money rental rates and hence credit-money aggregates, (c) alters capital requirements to alter the quantum of credit that financial institutions can emit in monetized form, or (d) employs a combination of such tactics.[84]

In all such cases, the hope is that Fed monetary easing will translate into greater bank lending to productive and other needful units throughout the national economy, or that counterpart monetary tightening will similarly contract credit-money aggregates and thereby slow inflationary spending activity. The problem is that the hope sometimes goes almost entirely unfulfilled and always goes less than fully fulfilled. The reason is not hard to find once one notes the pervasiveness of recursive collective action problems in any decentralized exchange economy and associated financial system like that of the U.S.[85]

During a bust, with prices falling, it is irrational for individuals to borrow and spend, even when the slump could be reversed were all individuals to borrow and spend simultaneously in concerted fashion. Such individuals lack the means of collective agency required to ensure that all individuals *do* engage in the requisite spending, however.[86] During a boom, in turn, with prices rising, it is likewise irrational for individuals *not* to borrow and spend, even when their all doing so inflates the bubbles that ultimately burst and become busts.[87] Private sector lending institutions are as caught up in this individually rational,

---

82. *See* sources cited *supra* note 72.

83. *See* sources cited *supra* note 72; *see also* Hockett, *Rousseauvian Money*, *supra* note 15, at 49.

84. Hockett, *supra* note 9, at 16–17; see also Hockett, *Capital Commons*, *supra* note 10; Hockett, *supra* note 31.

85. Hockett, *supra* note 19, at 17; *see also* Robert Hockett, *Recursive Collective Action Problems: The Structure of Procyclicality in Financial and Money Markets, Macroeconomies, and Formally Similar Contexts*, 3 J. FIN. PERSPS. 1 (2015) [hereinafter *Recursive Collective Action Problems*] (explaining what constitutes a recursive collective action problem and how to address those challenges).

86. *See* Hockett, *Recursive Collective Action Problems*, *supra* note 85.

87. *Id.* at 18.

collectively irrational logic as are their prospective borrowers.[88] A money-modulatory system that depends on the independently-reached decisions of such institutions will accordingly lack the means of collective agency required to conduct monetary policy efficiently.[89]

A similar individually rational, collectively irrational logic afflicts national investment in much productive industry and infrastructure.[90] Many productive projects, whose value-adds inure to the benefit of large populations over lengthy temporal durations, do not inure sufficiently to the benefit of individuals over short temporal durations to induce them optimally to engage or invest in the productive activity in question.[91] It is thus individually rational for disaggregated and uncoordinated persons simply to leave long-term value on the table, as collectively irrational as that is.[92] And once again, what is true of individuals here is likewise true of the disaggregated profit seeking, private sector institutions that lend to them, whose "short-termism" is individually rational under present disaggregated and uncoordinated arrangements, even while collectively wasteful and even disastrous in the longer term.[93]

These two collective action impediments to efficient money-fueled productive activity can be readily remedied by limiting the role of disaggregated middleman institutions in the monetary policy effectuation process, leaving them to retail lending against a backdrop of publicly modulated and hence stable money and credit aggregates economy-wide.[94] And a Fed-administered rendition of the IVL Plan affords ready means of doing just that—means of enabling the Fed fully to discharge its role as our polity's authorized collective agent in matters monetary.[95] This is readily demonstrated in respect both of monetary policy and of infrastructure investment policy.

The monetary policy case is the easiest to see in light of the foregoing schematization of digital IVL Accounts and associated digital dollars. All that the Fed needs do is: (a) pay interest on IVL Accounts; (b) raise those rates to slow down, and lower them to speed up, spending activity by account holders; and (c) in extreme cases, either impose negative interest rates upon, or conduct direct digital helicopter drops into, these same accounts. And that would be that—direct, leak-proof monetary policy,

88. *Id.* at 18–19.

89. *Id.* at 19.

90. *See* Hockett, *Capital Commons*, *supra* note 10, at 33–38; *see also* Hockett, *Recursive Collective Action Problems*, *supra* note 85, at 20.

91. *See* Hockett, *Recursive Collective Action Problems*, *supra* note 85, at 20; *see also* Hockett, *supra* note 11.

92. *See* Hockett, *Recursive Collective Action Problems*, *supra* note 85, at 20.

93. *See* sources cited *supra* note 72; *see also* Robert Hockett & Saule Omarova, *Private Wealth and Public Goods: A Case for a National Investment Authority*, 43 J. CORP. L. 437 (2018).

94. *See* Hockett, *supra* note 9, at 18.

95. *Id.* at 16.

and associated effectuality where expansionary and contractionary policy alike are concerned.[96]

The investment policy case is slightly more complicated than is the monetary policy case, if only because the necessary architecture in this case has not already been fully laid out as it was for the monetary policy case earlier in this Article. It is nevertheless easy enough to describe quickly what is needed and then diagram the result. The key point to remember is that the Fed, like any financial institution, maintains a large and complex balance sheet comprising many classes of assets and many classes of offsetting liabilities. The Fed uses this balance sheet somewhat in the way that Congress uses the Internal Revenue Code—as a means of policy-optimal macro-allocation economy-wide.[97]

Among the Fed's liabilities are the Reserve Accounts that it maintains for private sector banking institutions, which operate much as do individuals' deposit accounts maintained with these private sector banks themselves. Among the Fed's assets, in turn, are the trillions of dollars' worth of Treasury securities, mortgage and other federal agency securities, and International Monetary Fund (IMF) Special Drawing Rights (SDRs) that it holds—not to mention the new assets newly acquired pursuant to the Fed's pandemic relief efforts.[98] Private sector bank balance sheets look much like the Fed's balance sheet, save that the assets and liabilities include much more in the way of for-profit private investments and individual demand deposits, respectively, than does the latter.[99] Migrating an IVL-like digital wallet system from Treasury to Fed would involve adding wallets to the liability side of the balance sheet in a manner well integrated with the addition of new assets to the asset side of the balance sheet. It would look, more or less, as follows.

B. *How We Might Migrate*

As with the Treasury Direct Plan laid out above, so here with the Fed rendition there would be both functional and technical requirements to discharge. I will address them in the same order here as I did above.

1. Functional Requirements

The functional requisites to migration of the kind here contemplated fall into two categories. First come the functionalities of the system *qua* payments system, which are identical to those laid out above in Part II in connection with the Treasury Direct Plan. Second come the

96. *Id.* at 18.

97. *Id.*

98. *See* Hockett, *supra* note 49, at 20 (elaborating on the new assets now being acquired pursuant to the Fed's pandemic relief efforts).

99. *See id.* at 24–25.

functionalities requisite to incorporating the Fed version of the plan into its regular monetary policy operations. Those are unique to the Fed rendition of the plan, so let us now turn briefly to carefully elaborating them.

A FedWallet rendition of the IVL Plan would simply alter the compositions of the Fed's own and private sector banks' balance sheets in a few straightforward ways. First, the Fed IVL Master Account would simply be (a large portion of) the liability side of the Fed's balance sheet. Payments among businesses and individuals would then manifest as shifting allocations on that liability side of the Fed balance sheet (see Figure 5, below). Insofar as individual Fed IVL wallet accounts subsumed within that Fed IVL Master Account were employed in this manner as transaction accounts by their holders, there would also be a corresponding reduction in the sizes of private sector bank balance sheets. This would depend on what ceilings, if any, we imposed upon wallet account balances. Their deposit liabilities would migrate in some measure over to the Fed.[100]

Second, insofar as we wanted private sector banks to continue to "gate-keep" in connection with business and other forms of productive lending as they do now—when not betting on price movements on secondary financial and tertiary derivative markets—we would permit them to do so in either or both of two ways. The first way would be by letting them offset their lending with such ordinary deposits as they can continue to attract or legally open. They might then elect to sell, as they do now, some of these loans on to the Fed *ex post* as they now often do to other federal entities such as the Government-Sponsored Enterprise (GSE).[101]

The second way would be by letting them borrow from the Fed *ex ante* or *ex post* through the Fed's Discount Window in connection with loans they either plan to extend or have extended—a sort of bespoke lending rendition of what the Fed, Fannie Mae and other GSEs, and other entities do in purchasing and thus monetizing bonds, notes, and other issuances.[102] In all such cases, the effect would be simply to substitute liabilities owed to the Fed for liabilities owed to individual depositors on bank balance sheets, and add these bank liabilities to the asset side of the Fed's balance sheet, thereby offsetting the new Fed Note equivalent liabilities that the Fed "owes" in the form of business and individual IVL wallet accounts.[103]

---

100. *Id.* at 20.

101. *Id.*

102. *Id.*; *see also* Hockett, *Capital Commons*, *supra* note 10 (detailing, in particularly painstaking detail, the many accounting implications of these operations).

103. *See* Hockett, *supra* note 49, at 20. The scare-quotes around 'owes' are because these liabilities stem from, rather than preceding and enabling, Fed loans to the 'creditors.'

Were we to go this route, requiring private sector banks to fund some or all of their investments through Fed Discount Window lending instead of privately maintained deposits could have as salutary an effect upon national investment policy as the Fed's maintaining a system of IVL FedWallet accounts for all legal persons would have upon national monetary policy.[104] For the Fed now could *condition* its lending expressly upon private sector banks' lending for manifestly *productive* purposes in primary markets rather than upon speculative activity in secondary and tertiary markets. In effect, we would then have both (a) a renewed—and far more effective—Glass-Steagall separation of depository from speculative financial market activity, and (b) an affirmative linkage of that depository activity to productive investment.[105]

Another asset side offset to the new currency-like liabilities that the Fed would take on in maintaining a system of IVL FedWallet accounts for businesses and individuals would be direct Fed purchases of infrastructure bonds, "social impact" bonds, state, and municipal securities (munis),[106] and issuances made by any new public entity we might establish in future to plan and conduct national development finance. The possibilities here are quite breathtaking in some cases, but their details are beyond the scope of this Article and accordingly more fully discussed in other work complementing this one.[107]

2. Technical Requirements

The technical prerequisites to digitizing Fed administered digital dollars and IVL wallets are, like the functional requirements other than monetary policy requirements, the same here as in the Treasury case. In other words, the same "Accounts," "Payments," "API," and "Ledger" layers discussed in Part II above would have to be dealt with here in designing and instituting a Fed IVL platform for value- storage and

104. *See* Hockett, *supra* note 49, at 6; *see also* sources cited *supra* note 72.

105. *See* Hockett, *supra* note 49, at 11; *see also* sources cited *supra* note 72.

106. *See* sources cited *supra* note 105. For more of this author's work on the Fed's new Municipal Liquidity Facility (MLF) and QE, see Memorandum from Robert Hockett, *The Fed's Municipal Liquidity Facility: Present and Future Necessities and Possibilities* (May 10, 2020) (on file with author), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3597732 [https://perma.cc/5ZH3-E4SL]; Robert Hockett, *Community QE2: Newly Eased Terms and a New Game Plan For Use*, FORBES (May 2, 2020, 8:35 AM), https://www.forbes.com/sites/rhockett/2020/05/02/community-qe2-newly-eased-terms-and-a-new-game-plan-for-use/ [https://perma.cc/ QVU8-H4VV]; Robert Hockett, *Community QE - An April Game Plan for States and Cities*, FORBES (Apr. 12, 2020, 8:39 AM), https://www.forbes.com/sites/rhockett/2020/04/12/community-qean-april-game-plan-for-states-and-cities/ [https://perma.cc/PC5S-XRPJ]; Robert Hockett, *Welcome to Community QE - Now Let Us Put It to Use*, FORBES (Apr. 9, 2020, 10:21 AM), https://www.forbes.com/sites/rhockett/2020/04/09/welcome-to-community-qe/ [https://perma.cc/GRL4-C6M7].

107. *See* sources cited *supra* note 106; *see also* sources cited *supra* note 72.

transfer. Because there is almost no difference between the two cases—Treasury and Fed—on this dimension. and because the same federal offices that would do the converting at Treasury can do it at the Fed, let us incorporate the findings of Part II here by reference as well.

The one difference between the two cases is that Treasury, unlike the Fed, already administers individual digital accounts for citizens, while the Fed only manages Reserve Accounts for large banking and other privileged financial institutions. The Fed would accordingly have to build out millions of IVL wallet accounts from scratch. Technically, of course, this need be no more daunting than it was for Treasury when it began Treasury Direct. Indeed, the Fed can even make use of the same personnel that the Treasury did when it turns to the task and can learn from any bugs or mistakes that the Treasury Direct project has by now brought to light. It will, however, take time.

C. *Pictographic Summation and Synthesis*

Diagrammatically, then, in going the Fed route for an IVL digital dollar we would move from a banking system like that depicted in Figure 3 to a banking system like that depicted in Figure 4 where credit-money flows and associated assets and liabilities are concerned. Adding the payment platform of the previous diagrams to Figure 4 yields a complete picture in the form of Figure 5, in connection with which the reader is hereby reminded that all entities represented above the Master Account box in the diagram are among the Account Holders, hence Payors and Payees, represented below that box in the diagram.

Figure 3: Current Fed/Bank/Depositor/Issuer Arrangements & Financial Flows

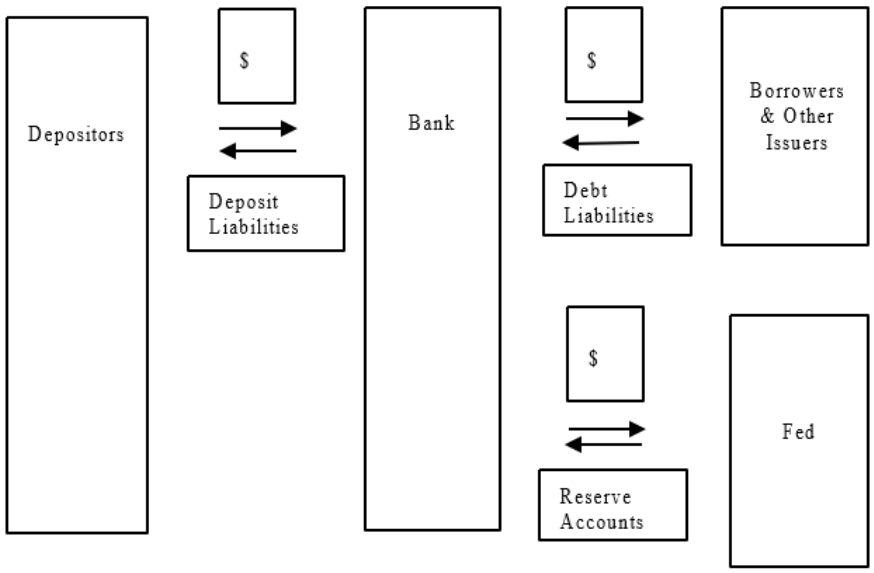


Figure 4: Reformed Fed/Bank/Depositor/Issuer Arrangements & Financial Flows

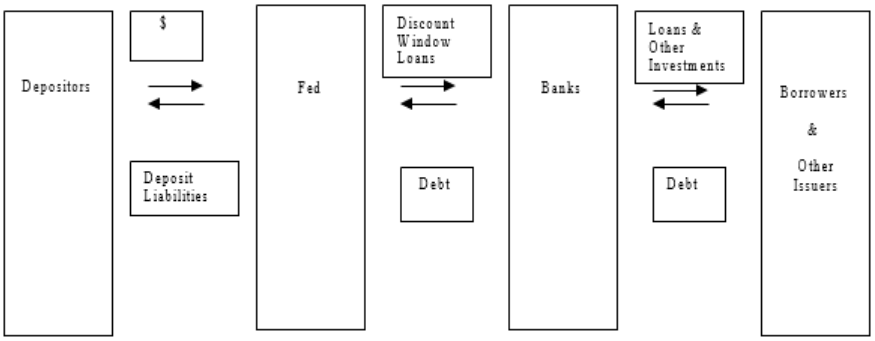
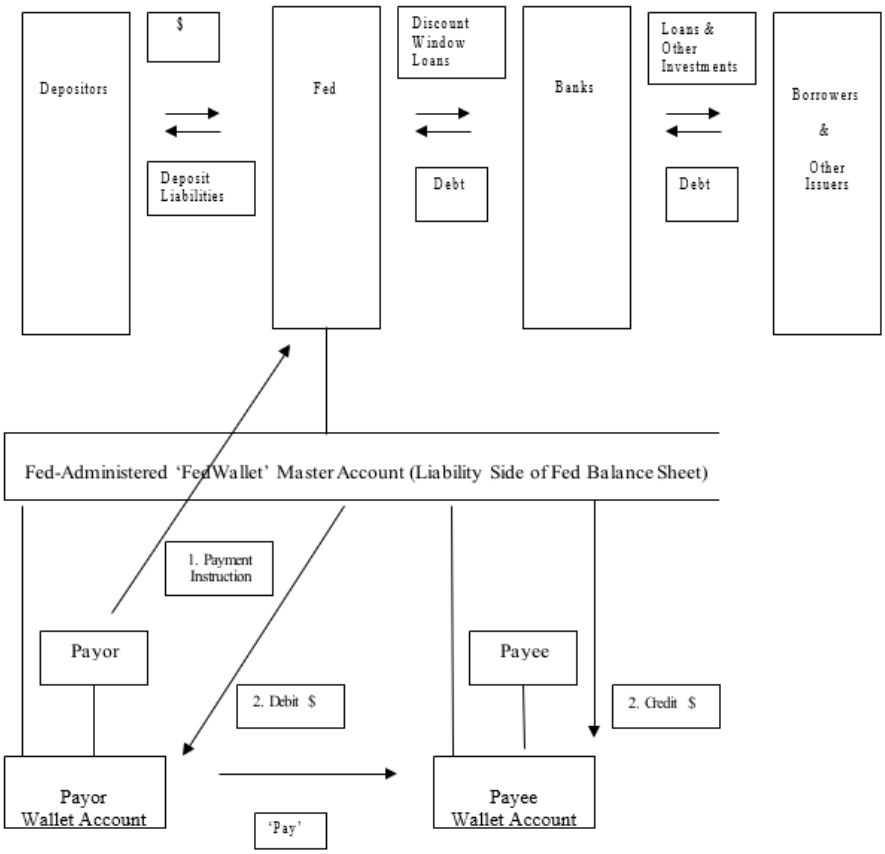


Figure 5: Reformed Fed/Bank/Depositor/Issuer Arrangements & Financial Flows, with Fed--Administered 'FedWallet' IVL Platform



CONCLUSION

The technology involved in the Treasury Direct upgrade, or even in establishing a FedWallet counterpart, will not be *trivial* to build, but neither will it be particularly *daunting* to build. It has been done before, by multiple firms and networks for multiple purposes, over the years. All that differs now is that we are doing this for a forthrightly public purpose—that of installing a universally accessible, fee-free and frictionless, state-of-the-art national value storage and payments architecture. As noted above, this is desirable in all times, not only times of crises. So, in doing this we will also be opening saving and paying to 50 million unbanked and underbanked households, businesses, and individuals in need of immediate aid during the current crisis and any subsequent crises.

As the discussion above has indicated, going the Fed route would be somewhat more complicated than going the Treasury route, and for that reason the Fed route is probably not up to the task of immediate implementation during the present pandemic. But in time it could be managed—particularly were we to start now at Treasury and then in future migrate to the Fed—as the Greenback paper dollar regime itself did in the late 19th and early 20th century. As noted above, central banks worldwide are already developing and rolling out CBDCs in the name of greater commercial inclusion, smoother payment systems, less leaky monetary policy, and financial stability.[108] Sweden began its first public trial of the e-Krona project, long in development, only last February. China will soon follow.

China is a particularly interesting case because it has begun more and more often to secure first mover advantages relative to the U.S. in multiple spheres of economic competition.[109] Is there really any reason—especially now, amid crisis—to cede China the advantage, or even global monopoly status, in this space as well? Surely there is not. Our present pandemic-fueled exigency requires we act quickly in any event, which TreasuryDirect makes quite feasible.

---

108. It bears noting that private sector entities are even now actively engaged in mastering the new technologies that lie behind what I propose here, thereby potentially 'disrupting' financial stability and accordingly affording us yet another reason to digitize the dollar now if we wish to avoid a digital rendition of the highly volatile 'wildcat currency' days that necessitated establishment of the Treasury-administered Greenback itself during the Civil War. See Hockett, *Capital Commons*, *supra* note 10; Hockett, *supra* note 31, at 228–30, for a full vetting of the subject.

109. *See* Robert Hockett, *America's Digital Sputnik Moment*, THE HILL (May 12, 2020, 8:00 PM), https://thehill.com/opinion/technology/497427-americas-digital-sputnik-moment [https://perma.cc/9HBW-CS5H].

APPENDIX: THE TREASURY DOLLAR ACT OF 2020

A BILL

To establish a uniform, publicly administered mechanism through which relief payments and other public sector disbursements can be made to all citizens, legal residents, and businesses legally operating within the territorial jurisdiction of the United States; and in so doing to provide the digital equivalent of a bank savings and transaction account to these same citizens, legal residents, and businesses.

Be it enacted by the Senate and House of Representatives of the United States of American in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the 'Treasury Dollar Act of 2020.'

SECTION 2. FINDINGS AND PURPOSE.

(a) FINDINGS.—Congress finds that—

(1)For over half a century from the mid-1860s into the early 20th century, the US Treasury issued the principal legal tender currency used in the United States to settle all obligations, public and private;

(2)After the Federal Reserve Note ('dollar bills') began first to supplement, then to supplant Treasury currency as the nation's principal legal tender in the second and third decades of the 20th century, Treasury currency continued—and continues—to qualify as legal tender;

(3)The Treasury continues to issue trillions of dollars' worth of other US sovereign liabilities—including Bills, Bonds, and Notes—which constitute the largest securities market in the world;

(4)The Treasury is both legally and logistically well positioned to issue any

new sovereign liabilities, including zero-coupon, dollar denominated liabilities counting as legal tender, in whatever quantities Congress sees fit to authorize, be this *ad hoc* in crises or on a continuing basis;

(5)The Treasury also maintains a system of 'Treasury Direct' accounts open to all citizens and legal residents of the United States, through which account-holders can transact in Treasury securities with the Treasury '24/7,' any time day or night;

(6)The United States is in need of a universally inclusive and efficient, 'real time' means of transmitting purchasing power to citizens, legal residents, and businesses that suffer the income and liquidity consequences of crisis-wrought monetary, financial, and macroeconomic contraction;

(7)Any such system as that just described would be both more just and more growth-promoting than any less inclusive or less efficient system can be, because (a) a value storage and transfer architecture—that is, a savings and payment platform—is an essential public utility in any commercial society or exchange economy such as those of the United States, and (b) economic growth is measured by transaction volume, while transaction volume is a positive function of transaction velocity;

(8)Millions of citizens and legal residents of, and small businesses operating in, the United States have limited or no access to traditional banking and payments services of the kind necessary both to transact with each

other and to receive income support, tax refunds, program and procurement payments, or other disbursements from the federal fisc, leaving these citizens, legal residents, and small businesses vulnerable to the exploitative practices of many payday lenders and payment service firms.

(b) PURPOSE.—The purpose of this Act is to build upon the historical precedent and institutional architecture referenced in Findings (1) through (5) in order to rectify the deficiencies identified in findings (6) through (8).

SECTION 3. DEFINITIONS.

(a) Account.—
(b) Account Holder.—
(c) Bank Account.—
(d) Banking Association.—
(e) Banking Services.—
(f) Coupon.—
(g) Credit and Debit Card.—
(h) Cryptographic.—
(i) Digital.—
(j) Digital Account Wallet.—
(k) Digital Equivalent.—
(l) Digital Payment System.—
(m) Digital Wallet.—
(n) Disbursements.—
(o) Dollar.—
(p) Dollar Bill.—
(q) E--Banking.—
(r) Electronic Banking.—
(s) Federal Reserve Note.—
(t) Interest.—
(u) Interoperability.—
(v) Issuable.—
(w) Legal Tender.—
(x) Payday Lender.—
(y) Payment Service.—
…

SECTION 4. TREASURY DOLLARS.

Congress shall authorize and instruct the Department of the Treasury to issue a new class of Treasury Bill, to be designated a 'Treasury Dollar Bill,' abbreviated as 'Treasury Dollar.' Treasury Dollars shall—

> (a) Be valued at precisely one Federal Reserve Note (colloquially known as 'the dollar bill') per Treasury Dollar, yielding no interest or 'coupon' that Federal Reserve Notes do not, and differing from Federal Reserve Notes only in respect of their issuer;
>
> (b) Be designated as Legal Tender, sufficient to discharge all payment obligations, public and private, on precisely the same terms as Federal Reserve Notes;
>
> (c) Be issuable in both paper and digital form, and any other form in which Federal Reserve Notes are or shall in future be issued;
>
> (d) Serve as the unit of account in Treasury Direct Accounts as specified in Section 5 of this Act.

SECTION 5. TREASURY DIRECT ACCOUNTS.

Congress shall authorize and instruct the Department of the Treasury to expand its existing system of Treasury Direct Accounts in the following three manners—

> (a) Bank and Thrift Account Interoperability.—All Treasury Direct Accounts shall retain the interoperability with Bank or Thrift Transaction Accounts that they currently have, save that, pursuant to Section 4(b) of this Act declaring Treasury Dollars legal tender, there shall be no public or private sector requirement to convert Treasury Dollars into Federal Reserve Notes or their digital equivalent, or *vice versa*, as there presently is when transferring funds between Bank or Thrift Transaction Accounts and Treasury Direct Accounts in purchasing or redeeming

present-day Treasury Securities that are not Treasury Dollars;

(b) E--Banking, Phone Banking, Credit and Debit Card, Automatic Teller Machine, and Other Banking Services.—Pursuant to Section 4(b) of this Act declaring Treasury Dollars to be legal tender, no State or Nationally chartered Banking Association or Thrift Institution shall discriminate between Treasury Dollars and Federal Reserve Notes or their digital equivalent in administering the Electronic Banking ('e-banking'), Phone or Other Device Banking, Credit and Debit Card, Automatic Teller Machine (ATM), or other traditional banking services that they offer customers;

(c) Digital Account Wallets.—The Treasury shall, with all deliberate speed—

(1) Add digital peer-to-peer ('P2P') Interoperability to all Treasury Direct Accounts, enabling all Account Holders to transact directly in real time both with the Treasury and with one another, so that Account Holders without Savings or Transaction Accounts held with other institutions, including Banking Associations and Thrift Institutions, can transact directly both with Treasury and with one another in 'real time' through their Treasury Direct Account Wallets;

(2) Retain the services of the US Digital Service to design the P2P-- Interoperable Digital Account Wallets referenced in Subsection (c)(1) of this Section immediately above;

(3) Cryptographically build into the Digital Account Wallet system all Privacy and 'Hack-Proofing' protections that Treasury Direct Accounts currently offer or that Banking

> Associations and Thrift Institutions are currently required by law to provide in connection with the Transaction Accounts and Payment Services that they provide.

(d) Treasury Disbursements into Digital Account Wallets.—After the system of Digital Account Wallets described in Subsubsection (c)(e) of this Subsection is operational, Treasury shall make all future digital or electronic disbursements, including but not limited to crisis relief payments, into these Account Wallets, with the object of encouraging wide use of this system as the preferred, universally accessible digital payments platform for all e-payments made in the United States.

DEFENDING FACE-RECOGNITION TECHNOLOGY (AND DEFENDING AGAINST IT)

Henry H. Perritt, Jr.[*]

I. INTRODUCTION 42

II. TECHNOLOGY OF FACE-RECOGNITION 45
A. *Machine Learning* 46
B. *Bases for Comparisons* 49
1. Probe Images 49
2. Training Databases 50
3. Enrolled Databases 51
4. Searching 52
C. *Accuracy* 52
D. *Speed of Processing* 54

III. USES IN LAW ENFORCEMENT 55
A. *Permutations* 56
B. *Narrowing the Class of Suspects* 57
C. *Supplementing Eyewitness Identification* 58
D. *Corroboration by Other Forensic Techniques* 59
E. *Field Identification* 59
F. *Booking Arrestees* 60
G. *Scanning Crowds to Find Fugitives* 61
H. *Artist Reconstructions* 62
I. *Law Enforcement Products in the Marketplace* 62

IV. LEGAL ANALYSIS 65
A. *Caselaw and Commentary* 67
B. *Privacy Concerns: Separating the Wheat from the Chaff* 68
C. *Federal and State Statutes* 71
D. *Constitutional Limitations* 74
1. Confrontation Clause 74
2. Excluding Basis of Testimony Under *Williams v. Illinois* 78
3. Computerized Face-Matching as Basis for Testimony 85

* Professor of Law (retired) and former dean, Chicago-Kent College of Law. Member of the bar: Virginia, Pennsylvania, District of Columbia, Maryland, Illinois, Supreme Court of the United States. Author of more than 100 articles and twenty-five books on dispute resolution, technology and law, and labor law. Commercial helicopter and private instrument airplane pilot. Extra class radio amateur (K9KDF). The author appreciates the insights of his former student, Zack Beaver, who served as a Trooper and Sergeant of the Indiana State Police before he became a lawyer.

4. Fourth Amendment 87
a. Acquiring DNA 88
b. Acquiring Fingerprints 89
c. Acquiring Photographs 91
d. Patterns of Movement 92
e. Incident to Arrests 93
E. *Challenging Reliability of Traditional Witness Identification* 93
1. Suggestiveness 97
2. Adjudicating Suggestiveness 106
3. Wanted Posters 109
F. *Challenging Scientific Methods of Identification and the Experts Presenting Them* 110
1. Expert Witnesses 110
2. Voir Dire 111
3. Admissibility of Science 111
4. Specific Challenges to Comparisons 112
5. The Less Human Involvement, the Greater the Reliability? 117

V. CHALLENGING COMPUTERIZED FACE-RECOGNITION EVIDENCE 120
A. *Expert Testimony* 120
1. Voir Dire: Qualifying Experts 121
2. Application of Reliable Principles: Frye or Daubert 122
3. Authentication 124
B. *Principles for Defendant Access to Face-Recognition Technology* 124
C. *Questions to Ask* 124
1. Limitations of the Technology 125
2. Face-Recognition Trial Tactics 127
3. Sample Questions 128
D. *Trade Secret Objections* 132

VI. LIMITING USE OF FACE-RECOGNITION BY LAW ENFORCEMENT 134
A. *Considerations* 134
B. *Focusing on What Can Go Wrong* 137
C. *Draft Statute* 138

I. INTRODUCTION

Drew Williams and Michael Thompson met for the first time in a convenience store at 1:30 AM on a July night. Drew, a junior at the state

university, worked in the store to earn additional money. Michael also wanted additional money, but he did not want to work very hard to get it. Michael came into the store and looked around. Not seeing anyone else, he walked up to the counter, pulled out a pistol, and told Drew that he wanted all his cash. Drew argued briefly, assessing whether he could overpower the somewhat smaller Michael—but the pistol in Michael's hand more than evened the odds. "Don't shoot me," he said. "You can have everything in the register." Drew opened the cash register drawer and began taking bills out and putting them on the counter.

"The ones underneath the coin tray as well," Michael said. Drew lifted the coin tray and pulled out a small handful of 20s and one $100 bill and put them on the counter beside the rest of the cash.

"Now," said Michael, "open the safe."

"I don't know how to open the safe," Drew said. "I don't have the combination." He pointed at a sign that said, "Store personnel do not have the combination to the safe."

Michael looked at the sign, looked back at Drew, and pulled the trigger, shooting Drew in the chest.

Drew died before the ambulance got him to the hospital.

The police could find no witnesses, but the store had a surveillance camera, and the recording showed everything that happened, including a full-frontal image of Michael's face.

Exposed to breathless stories in the media and press about police use of face-recognition technology, viewers and readers might imagine that the police could run the surveillance image of Michael through a face-recognition computer system, obtain a match to an individual known to be Michael, arrest him, haul him into court, and show the jury the computer match, likely resulting in conviction.

That very rarely happens—yet. Instead, law enforcement investigators take the output of the face-recognition system, —usually in the form of several potential matches, scored as to probability—and use them as the basis for further investigation. They may use the computer-generated matches as a photo array[1] to present to witnesses. They may use meta-data about the subjects in the matches to determine who had opportunity, means, and motive to commit the crime. They may take fingerprints or DNA samples from suspects identified from face-recognition and search them against databases.

A good bit of hysteria exists about face-recognition technology and its potential to turn the United States into "a surveillance state like

1. A photo array is an arrangement of photographs presented to a witness, to see if she can identify the image of the perpetrator from among them. *E.g.*, Small v. State, 180 A.3d 163, 169–73 (Md. Ct. App. 2018) (describing construction and use of a photo array).

China," given that half the population already has images of its faces in one database or another.[2]

Despite their rhetorical excesses, aimed at getting attention and strengthening fundraising, some of the alarmists identify important benchmarks for the evolving law of face-recognition in criminal procedure. Most significantly, they argue that the law of evidence, particularly hearsay rules, and the Constitution, especially the Sixth Amendment's Confrontation Clause, should be interpreted to entitle a criminal defendant to know if face-recognition technology was used to build the case against him. He should be entitled, they argue, to know how the technology was used if it was. If the technology played a significant role in singling out the defendant for investigation, the defendant should be entitled to probe its role and, if the role was substantial, to probe the reliability of the technology used.

The commentators are right about all of this, so far. On the other hand, if face-recognition technology played only a minor role in the investigation, and if other evidence is sufficient independently to identify the defendant as the perpetrator, the defendant should not be able to turn the trial into a generalized debate on the evils of face-recognition technology as a threat to personal privacy.

Face-recognition technology promises enormous improvements in identifying criminals, while reducing the incidence of wrongful accusations. But fears of its potential misuse, fueled by speculation amounting to little more than science fiction, is leading to calls for its outright prohibition, which have been embraced by many state legislatures. This is not the solution. The solution is a broader understanding of how the technology works and greater transparency through criminal discovery, so that those accused of crimes based in whole or in part on the technology have a meaningful opportunity to test its accuracy through the adversary process. The same techniques that allow a criminal defendant to challenge eyewitness identification should be available to challenge computer identification.

The objection still exists that, even if a wrongfully accused defendant is officially acquitted, she has been put to great expense, reputational injury, and psychological trauma by accusation and arrest. This is true of any criminal accused, however, whether face-recognition technology played any role in the accusation. The remedy lies in existing measures to test probable cause for arrest, to afford pre-trial release through the bond presentment process, and to vindicate through grand juries and preliminary hearings.

---

2. *See* John Palfrey, *The Ever-Increasing Surveillance State*, GEO. J. INT'L AFFS. (Mar. 2, 2020), https://gjia.georgetown.edu/2020/03/02/the-ever-increasing-surveillance-state/ [https://perma.cc/UDG6-WCUF] (explaining how, similarly to China, the United States collects a significant amount of biometric information about its citizens).

This Article looks beneath the surface of attacks on face-recognition technology and explains how it can be an exceptionally useful tool for law enforcement, complementing traditional forensic evidence such as fingerprints and DNA. It punctures myths about the technology and explains how existing rules of criminal procedure, developed for other kinds of forensic evidence, are readily adaptable to face-recognition. It opposes across-the-board restrictions on use of face-recognition technologies and advocates a more sophisticated set of guarantees of defendant access to the information necessary to probe reliability of computerized face-matches. Defendants must have reasonable access to the details of the technology and how it was used so that they have a meaningful opportunity to inform the factfinder of doubts about reliability.

Part II explains the technology, starting with machine learning, which enables a computer to represent faces digitally based on their physical characteristics, so that they can be matched with other faces. This part also explains how shortcomings in the algorithms or training database of faces can produce errors, both positive and negative, in identification.

Part III explores existing and potential uses of face-recognition in law enforcement, placing the technology into the context of traditional police investigations.

Part IV summarizes the relatively sparse caselaw and the much fuller literature on face-recognition technology, in particular, evaluates claims of threats to privacy, and analyzes legal principles developed for analogous conventional criminal investigative and proof methods.

Part V constructs a legal framework for evaluating the probativeness of face-recognition technology in criminal prosecutions, develops strategies, and offers actual cross examination questions to guide defense counsel in challenging face-recognition technology.

Part VI acknowledges that some specific uses of the technology to scan crowds and streams of people may need judicial control and suggests a draft statute to assure such control.

II. TECHNOLOGY OF FACE-RECOGNITION

Face-recognition is an instance of pattern matching, which also includes voice recognition, natural language processing, text to speech conversion, auto-correction in word processing programs, and many video and audio compression algorithms.

Most of these types of pattern matching benefit from the use of machine learning techniques. The quality of what the machines learn depends on the size and representativeness of the exemplars fed into the machines during the learning process through a *training database*. The accuracy of the production system, —which, in the face-recognition context, seeks to match a *probe image* against entries in an *enrolled*

database—depends on the robustness of the statistical algorithms used to extract the distinguishing features.

A. *Machine Learning*

In machine learning, a large number of samples are processed by a digital computer.[3] Some of the samples contain the target image, and others contain something else. Thus, a robocowboy might be trained to recognize cattle by presenting hundreds of thousands of images of different kinds of animals, tagging only those that represent cows, bulls, steers, and calves.[4] Machine-learning techniques can be used to accommodate the challenges associated with recognizing the target image despite different orientations, different lighting conditions, and different backgrounds.[5] Machine learning works at multiple layers in face-matching applications. It learns what a face is; it learns how to reorient a facial image so that it more easily can be compared with others; it learns what features uniquely define a face; and it refines algorithms that can apply these steps to an arbitrary set of facial images in production systems.

The techniques work by scanning the lines of an image, much as a laser printer or office scanner does, and looking for discontinuities in brightness and color. A model of an image then can be constructed to identify the locations of those discontinuities.[6] Then, statistical techniques, enabled by a complex hierarchy of neural networks[7]

---

3. *See* U.S. Patent No. 20140105467A1, at paras. 0017–26 (identifying preceding face-recognition patents).

4. *See* Henry H. Perritt, Jr., *The 21st Century Cowboy: Robots on the Range*, 43 U. ARK. LITTLE ROCK L. REV. 149 (2020) (exploring feasibility of robot cowboy who herds cattle; describing machine learning aimed at recognition of cattle).

5. This involves the second step in most typologies: *alignment*. *See* Adrian Rosebrock, *Face Alignment with OpenCV and Python*, PYIMAGESEARCH (May 22, 2017), https://www.pyimagesearch.com/2017/05/22/face-alignment-with-opencv-and-python/ [https://perma.cc/8V6L-UQPX] (explaining alignment).

6. A line connecting the discontinuities represents an "edge" in the image, such as the edge of a cheek in a human face. *See Image Processing with Python: Edge Detection*, DATA CARPENTRY, https://datacarpentry.org/image-processing/08-edge-detection/ [https://perma.cc/5CHT-VRJC] (last modified Aug. 3, 2020) (explaining edges and edge detection in image processing).

7. *See* Divyansh Dwivedi, *Face Recognition for Beginners*, TOWARDS DATA SCIENCE (Apr. 28, 2018), https://towardsdatascience.com/face-recognition-for-beginners-a7a9bd5eb5c2 [https://perma.cc/EBJ9-HTYU] (explaining how neural networks can facilitate use of statistical techniques such as Principal Component Analysis, Linear Discriminant Analysis, Independent Component Analysis, Discrete Cosine Transforms, Gabor Filters, and Markov Models for face-recognition); ARUN ALVAPPILLAI & PETER NEAL BARRINA, Face Recognition USING MACHINE LEARNING (2017), http://noiselab.ucsd.edu/ECE285/FinalProjects/Group7.pdf [https://perma.cc/UU7L-GZ9D] (brief but formal paper on face-recognition algorithms).

implementing statistical algorithms, can compare the location of different types of discontinuities between images, and, thus, identify images that are most similar. The indicia of similarity are the particular facial features that discriminate a cow from a wolf—or one face from another.[8]

The "machine-learning" label applies to the process of identifying the distinguishing features that have statistical significance.[9] There is nothing magical about the analysis: it is factor analysis,[10] which has been used as a social science methodology for more than 100 years.[11] What has changed is computing power, the availability of digital storage, cheap digital cameras, and an enormous inventory of digital representations of faces.

The foundational layer examines a large inventory of images of faces (the *training database*) to learn what a face is.[12] This process is much like the one described for the robocowboy learning how to recognize a cow. The statistical model of a face then is tagged to identify those features that vary from one face to another, such as: spacing of the eyes, height of the forehead, thickness of the lips, width of the nose, coloration, and so on. Facial features could be identified and tagged in advance, by a knowledge engineer questioning people on how they recognize faces and

---

8. Adam Geitgey, *Machine Learning is Fun! Part 4: Modern Face Recognition with Deep Learning*, MEDIUM (July 24, 2016), https://medium.com/@ageitgey/machine-learning-is-fun-part-4-modern-face-recognition-with-deep-learning-c3cffc121d78 [https://perma.cc/266R-YDKX] (explaining the feature extraction step and that some commentators call this step identifying "landmarks").

9. One popular method is the Viola/Jones approach. *E.g.*, Paul Viola, *The Viola/Jones Face Detector* (2001), https://www.cs.ubc.ca/~lowe/425/slides/13-ViolaJones.pdf [https://perma.cc/Q9LD-JF2E] (explaining method with slides); Paul Viola & Michael Jones, *Rapid Object Detection Using a Boosted Cascade of Simple Features* (2001), https://www.cs.cmu.edu/~efros/courses/LBMV07/Papers/viola-cvpr-01.pdf [https://perma.cc/SL2P-YTW6] (describing a popular method of machine learning; more formal paper).

10. *E.g.*, *Factor Analysis*, STATISTICS SOLUTIONS, https://www.statisticssolutions.com/factor-analysis-sem-factor-analysis/ [https://perma.cc/9R9X-LB74] (last visited Jan. 11, 2021) (describing that factor analysis is a technique used to condense large amounts of variables into a lower amount of factors).

11. *See generally* Robert Cudeck, *Factor Analysis in the Year 2004: Still Spry at 100*, *in* FACTOR ANALYSIS AT 100: HISTORICAL DEVELOPMENTS AND FUTURE DIRECTIONS 1 (Robert Cudeck & Robert C. MacCallum, eds. 2007).

12. This is the "detection" step. *See* Oleksii Kharkovyna, *An Intro to Deep Learning for Face Recognition*, MEDIUM: DEEP LEARNING (June 26, 2019), https://laptrinhx.com/an-intro-to-deep-learning-for-face-recognition-3710804757/ [https://perma.cc/KZ2P-78VK] (identifying detection, alignment, feature extraction, and feature matching to database) as the steps in face-recognition); U.S. Patent No. 20140105467A1, at paras. 0009–15 (background of the invention, describing Detection, Alignment, Normalization, detection, alignment, normalization, representation, and matching steps in pattern matching); Geitgey, *supra* note 8 (describing and illustrating the steps with examples of actual faces of celebrities; providing links to Python programs that execute the algorithms).

know that an image is a face instead of something else. Human brain research shows that human beings pay most attention to eyes, cheekbones, nose, mouth, eyebrows, and texture and color of skin, when recognizing faces.[13]

Machine learning, however, does a better job because it identifies features, e.g., symmetry, that distinguish one face from another, which may escape the conscious notice of an individual observer, no matter how skilled. "The most appropriate approach is to enable the computer to determine the characteristics that need to be collected."[14]

At the conclusion of this layer of processing, the program has a template for a face. It now can take the image of a new face (the *probe face*) and determine the values for each of the facial features that have differentiating effects.[15] Most programs work with about 100 reference points that comprise individual features.[16] Then the computer software compares the faceprint of the probe face to the faceprints in the enrolled database.[17]

> The most important measurements for face-recognition programs are the distance between the eyes, the width of the nostrils, the length of the nose, the height and shape of the cheekbones, the width of the chin, the height of the forehead and other parameters. After that, the obtained data are

13. Kharkovyna, *supra* note 12; *see* Brendan F. Klare et al., *Suspect Identification Based on Descriptive Facial Attributes*, IEEE INT'L JOINT CONF. ON BIOMETRICS, https://ieeexplore.ieee.org/abstract/document/6996255 [https://perma.cc/S4QT-MMYR] (describing matching algorithm developed using crowd-sourced specification of 46 face attributes as basis for machine learning, by the co-founder and CEO of Rank One Corp.).

14. Kharkovyna, *supra* note 12.

15. *See, e.g.*, U.S. Patent No. 5,859,921 (issued Jan. 12, 1999) (describing apparatus that takes a facial image, corrects for lighting differences, and detects eyes).

16. *See* U.S. Patent No. US20140105467A1, at para. 0009:

> There are about 80 nodal points on a human face. A few of the nodal points that are measured by the FACEIT software are: distance between eyes; width of nose; depth of eye sockets; cheekbones; jaw line; and chin. These nodal points are measured to create a numerical code that represents the face in a database. This code is referred to as a faceprint and only fourteen to twenty-two nodal points are necessary for the FACEIT software to complete the recognition process.

17. *See* Scott Jeffrey Klum, *Facesketchid*: *A System for Facial Sketch to Mugshot Matching 3* (2014) (Master's Thesis, Michigan State University), http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.458.9523&rep=rep1&type=pdf (describing different methods for generating composite images: artists sketch from witness identification, computer-generated composition from witness description, and artist sketch based on surveillance photo).

> compared with those available in the database, and, if the parameters coincide, the person is identified."[18]

The feature measurements can be expressed as a "feature vector," or "faceprint," which represents a particular face.[19] The process concludes, as the quote says, with an additional layer of processing: comparing the features of a probe face with the features of faces in the database.[20]

As the discussion suggests, two different databases generally are used: the training database and the database of enrolled users. The training database likely would not relate to an ultimate law enforcement application. It would comprise an extremely large set of faces that are selected to represent the demographic characteristics of a population. This database is used for learning features that distinguish different faces. The database of enrolled users, in the law enforcement context, would contain faces of persons that might be of interest: from mugshots, driver's license photos, or passport photos. The actual matching is done between the probe photo and the enrolled user database.

Application in the law enforcement context is obvious. An unknown subject can be identified by matching a picture of his face with those in an enrolled database.

B. *Bases for Comparisons*

Face-matching involves comparing probe images against a database containing face images. Two databases are relevant to face-recognition: a training database and an enrolled database. Machine-learning algorithms are applied to the training database to find the features that identify a face and distinguish it from all others. This step develops the values to be used in the algorithms comprising a production face-matching system. The enrolled database is used in production systems to determine if the probe image matches an entry in the enrolled database, thereby permitting the system to output identifying data of the person with the matching face.

1. Probe images

Face-recognition, like the other two popular biometric techniques—involving fingerprints and DNA—depends upon a high-quality starting

---

18. Kharkovyna, *supra* note 12; *see also* Divyansh Dwivedi, *Face Recognition for Beginners*, TOWARDS DATA SCIENCE (Apr. 28, 2018), https://towardsdatascience.com/face-recognition-for-beginners-a7a9bd5eb5c2 [https://perma.cc/D4RD-LGTM] (presenting computer program in the Python language that performs the basic steps).

19. U.S. Patent No. 20140105467A1, at para. 0034 (explaining feature vector).

20. *See, e.g.*, *id.* (method and system for matching unknown facial image to image of celebrity by finding, comparing, contrasting, and identifying similar facial characteristics).

point: a clear image of a fingerprint, a sufficient quantity of uncontaminated DNA, or the image of a face at an orientation and with sufficient resolution that its features can be identified and measured. The most common limitation on useful computerized face-recognition is a poor quality[21] probe image, which often is the case with surveillance video. The most significant limitation on automated fingerprint matching is the poor quality of latent prints.[22] The most significant limitation on computerized DNA matching is the unavailability of a sufficient quantity of uncontaminated DNA to be the probe.

2. Training Databases

Acceptable accuracy for face-recognition requires a large number of digitized images of faces—in the hundreds of thousands or millions.[23] Only with a sufficiently large sample of different faces in the leaning database can the algorithm learn which features distinguish the different faces.[24] But this only needs to be done once. After the program has learned the distinguishing landmarks, it then can assign values to them for all the faces in an enrolled database, and then the system is ready to perform a search with respect to a probe face. The program simply takes the measurements of landmarks in the probe face and compares those with the corresponding measurements for each face in the enrolled database. It is not necessary to re-evaluate the training database each time a search is run.

Criteria for images to be included in the training database are quite different from the criteria for those to be included in the enrolled database. The training database is better if it includes the widest possible variety of faces, in the widest possible variety of orientations, lighting, and background. It also must include a variety of facial expressions, such as smiles, squints, and frowns.

The face-recognition system needs to learn how to identify an image comprising a face, and it needs a variety of visual backgrounds to be able to do that. It needs to handle faces in profile as well as full front orientation. It must not be stymied by different lighting conditions. The

---

21. "Poor quality," as the term is used in this Article, refers to more than the technical quality of an image—lighting, resolution, and focus. It refers also to factors that might obscure the subject's face, such as wearing a hood or a mask; the shot being taken from an angle rather than straight on; or rapid movement, which blurs the image in single frames comprising the video.

22. In criminal justice usage, "latent" means found in the field, as at a crime scene, rather than in a controlled environment, as with fingerprints taken as a part of the booking process. Latent does not refer, as in common usage, to whether the prints are apparent or hidden, requiring special techniques to expose them. *See* United States v. Baines, 573 F.3d 979, 982–983 (10th Cir. 2009) (explaining difference between latent and known fingerprints).

23. Klum, *supra* note 17, at 21–25 (describing training process for face-recognition algorithm).

24. The bigger the database, the greater the likelihood that it will contain a matching face.

machine learns how to normalize an image identified as a face, so that the production system can match the full-frontal equivalents of a diversity of orientations, lighting conditions, and expressions.

The training database also must include diverse sexes, ages, races, and ethnicities. A system trained only with African American faces is not going to do very well in recognizing Caucasian or Asian faces. A system developed from a training database without many Asian faces in it will do worse when identifying Asian targets. One that does not have many elderly faces will not do a good job recognizing older faces. The best training databases are as diverse in racial and demographic characteristics as the population.

With more diverse demographics, and greater variety of lighting conditions, orientations, and expressions, the training database will produce more robust algorithms—the quality of the eventual matches obtainable from their use will increase.

A number of commercial vendors and research labs have already created training databases that enable the deployment of commercial products into the marketplace that search and match faces, using enrolled databases specified by the customer.

3. Enrolled Databases

The enrolled database has a different purpose and, therefore, must be designed differently from the training database. The enrolled database should contain high-quality images of known persons.[25] The most common enrolled databases used in law enforcement are state collections of mugshots, driver's license photographs, and federal collections passport photographs, or more.[26] The images in these databases typically are full frontal (most mugshots also include a profile), have standard lighting, and the subject bears a serious expression. Search images easily can be expressed as a faceprint vector that unambiguously represents each face. A robust face-matching algorithm can take an equally high-quality probe image and determine if it matches. Then, the reliability of the face-matching depends only on the quality of the probe image.

Clearview AI, discussed in Section III.A, stands out from other products in that it also uses faces "scraped" from Facebook and other social media.[27]

---

25. *But see* discussion *infra* Section III.A regarding unknown to many-unknown matching.

26. Federal databases might be more comprehensive because, often, as a condition to receiving funds, agencies must report and provide data to the Feds. "The Feds almost always had access to better interstate data for this type of thing." E-mail from Zach Beaver, Esq., former Indiana State Police Sergeant, to author (June 8, 2020) (on file with author).

27. Scraping is the process of automatically searching the Internet, copying everything recognized as an image of a face, and storing it in the database. *See generally What Is Web*

Facebook simplifies its search by initially searching a new face only through the database of the friends of the person posting the new image.[28] In other words, the enrolled database for each search is small, and the probe face is highly likely to be in the database. Facebook's training database, conversely, is huge, comprising a substantial portion of all Facebook users.

4. Searching

Computers do not search databases by comparing every element of an entry of the search term with every element of each entry in the database. That would take far too long. Instead, search algorithms construct indices of the database entries, construct a similar index for the search term, and search for a match.[29] Once an index match is found, the algorithm may then go deeper and search for a match of data elements among a much more limited set of entries that all have the same index. The process is much like an index used by a large law firm, which presents a user with alphabet entries corresponding to the first letter of a lawyer's last name.

Index-based searching risks false negatives if the true match was mis-indexed. Superficially, criminal defense counsel is not concerned with false negatives because that means a potential guilty party got away. But if she defends on the ground that someone else did it, a face-match with someone else would be extremely valuable.

C. *Accuracy*

The National Institute for Standards and Technology (NIST) commissioned a series of tests and reports on face-recognition products.[30]

Scraping?, SCRAPINGHUB, https://www.scrapinghub.com/what-is-web-scraping/ [https://perma.cc/S5AR-NCN7] (last visited Dec. 2, 2020).

28. *See* discussion *infra* Section IV.C (explaining the Facebook face-matching algorithm).

29. *See* Henry H. Perritt, Jr., DIGITAL COMMUNICATIONS LAW § 1.03[C][1] (6th ed. 2020) (explaining the need for index-based searching in Internet routers); Tim Miller, *How Does Indexing Work*, CHARTIO, https://chartio.com/learn/databases/how-does-indexing-work/ [https://perma.cc/95DT-HHE9] (last visited Dec. 2, 2020) (explaining the need for indexes to make searches more efficient); Kenneth R. Moses, *Automated Fingerprint Identification System*, *in* FINGERPRINT SOURCEBOOK 6–29 (Alan McRoberts ed., 2011), https://www.ncjrs.gov/pdffiles1/nij/225326.pdf (explaining the need for indexing in automated fingerprint matching systems).

30. *See Facial Recognition Technology (Part III): Ensuring Commercial Transparency & Accuracy: Testimony Before the Subcomm. on Oversight and Reform of the H. Comm.*, 116th Cong. 54 (2020) (statement of Charles H. Romine, Director, Information Technology Laboratory, National Institute of Standards and Technology, United States Department of Commerce), https://www.nist.gov/speech-testimony/facial-recognition-technology-part-iii-ensuring-commercial-transparency-accuracy [https://perma.cc/SR8K-RXVT] (reporting on results of NIST program for testing reliability of commercial face-recognition products and summarizing errors associated with race and demographic groups).

Overall, the tests and reports showed error rates as low as 0.2%.[31] Experimentation with monkeys (simulating human experts) suggests that automated face-recognition systems can be more accurate than humans in some situations.[32]

Accuracy at this level can reduce wrongful convictions because the technology is more accurate than lineups,[33] in-court identifications, or on-scene descriptions identifying suspects as perpetrators of crimes.

The reliability of a face-matching algorithm depends importantly on the number of landmarks representing each face. If a system represents a face only by the distance between the pupils of the eyes, it would not be at all reliable, no matter how many faces are in its database. Too many different faces have similar distances between the eyes. Reliability improves as additional distinguishing features are added.

As with any statistical analysis, the computer programs applying them can report measures of reliability, e.g., 99% certainty that the face is a match or, say, only a 55% probability.[34]

The NIST report gave advice on use of face-recognition products that is pertinent to the criminal justice context:

> While publicly available test data from NIST and elsewhere can inform owners, it will usually be informative to specifically measure accuracy of the operational algorithm on the operational image data, perhaps employing biometrics testing laboratory to assist. Since different algorithms perform better or worse in processing images of individuals in various demographics, policy makers, face-recognition system developers, and end users should be

31. Patrick Grother et al., *Ongoing Face Recognition Vendor Test (FRVT) Part 2: Identification*, NAT'L INST. STANDARDS & TECH., https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8238.pdf [https://perma.cc/ZH6V-NBPX] (detailing recognition accuracy for 127 algorithms from 45 developers; concluding that "with good quality portrait photos, the most accurate algorithms will find matching entries, when present, in galleries containing 12 million individuals, with error rates below 0.2%; finding that face-recognition has undergone an industrial revolution, with algorithms increasingly tolerant of poor quality images).

32. Kharkovyna, *supra* note 12; P. Jonathon Phillips et al., *Face Recognition Accuracy of Forensic Examiners, Superrecognizers, and Face Recognition Algorithms*, 115 PROCEEDINGS NAT'L ACAD. SCI. 6171 (2018), https://www.pnas.org/content/115/24/6171 [https://perma.cc/J7XJ-PAN6] (reporting empirical data showing computerized face-recognition better than the median expert human).

33. A lineup is a live presentation of multiple individuals to a witness. The witness looks at the participants, sometimes hears them speak, and potentially identifies a perpetrator. Lineups are typically conducted in controlled environments such as a police station. *E.g.*, *What Are the Rules for Police Lineups?*, HG.ORG, https://www.hg.org/legal-articles/what-are-the-rules-for-police-lineups-35166 [https://perma.cc/3FSW-26DD] (last visited Dec. 3, 2020).

34. *See* U.S. Patent No. 20180373958A1 (filed Aug. 30, 2018) (describing statistical method for reporting reliability of computerized face-match).

> aware of these differences and use them to make decisions and to improve future performance. We supplement this report with more than 1200 pages of charts contained in seventeen annexes that include exhaustive reporting of results for each algorithm. These are intended to show the breadth of the effects, and to inform the algorithm developers.[35]

A separate NIST report evaluated the variability of accuracy with different demographic groups.[36] It reported "a wide range in accuracy across developers, with the most accurate algorithms producing many fewer errors."

Additionally, the report stated the following:

> With domestic law enforcement images the highest false positives are in American Indians, with elevated rates in African American and Asian populations; the relative ordering depends on sex and varies with algorithm. We found false positives to be higher in women than men, and this is consistent across algorithms and datasets. This effect is smaller than that due to race. We found elevated false positives in the elderly and in children; the effects were larger in the oldest and youngest, and smallest in middle-aged adults.[37]

Specific changes in algorithms can reduce bias.[38] Lower reliability of particular products for certain ethnic groups and ages should be fodder for effective cross examination. Competent counsel who understands the technology can perform effective cross examination of the proponents of the identification.

D. *Speed of Processing*

Computers are fast, but they still require finite amounts of time to do their work. Computer scientists estimate how long an application will take to produce its output by quantifying the duration of each step in the program and multiplying it by the number of times that step must be performed. Analyzing a new face requires computing the 100 or so landmarks and organizing them in a vector comprising the face-map. The

---

35. PATRICK GROTHER ET AL, *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*, 8280 NISTIR 3 (Dec. 2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf [https://perma.cc/XJ6M-QM8B]; *see also* Klum, *supra* note 17, at 32; *id.* at 38 (describing surveillance-photo to composite to matching results for Tamerlan Tsarnaev).

36. *See* GROTHER ET AL., *supra* note 35.

37. GROTHER ET AL., *supra* note 35, at 2.

38. ALEXANDER AMINI ET AL., *Uncovering and Mitigating Algorithmic Bias through Learned Latent Structure*, AIES (Jan. 2019), https://www.aies-conference.com/2019/wp-content/papers/main/AIES-19_paper_220.pdf [https://perma.cc/479D-N556].

time necessary for each computation must be multiplied by the number of landmarks—100 in this example.

Once the new face has been processed, it can be used as a probe image and compared with each of the images in an enrolled database. The time required for the search is directly proportional to the number of faces in the enrolled database. If multiple probe images are used, the search time increases in direct proportion to the number of probe images: searching for a match of three probes takes three times as long as a search for a match of one probe.

Thus, practical face-matching is not an instantaneous process, a characteristic limiting its application to large groups, the application that most concerns privacy watchdogs.

III. USES IN LAW ENFORCEMENT

Eventually, face-recognition technology will be powerful enough that a law enforcement agency can use face-recognition by itself to identify a perpetrator and to persuade a jury to convict him. For now, however, the technology is not that powerful. It is understood best as a complement to other forensic techniques, especially other biometric techniques such as fingerprint and DNA matching. Often, a computerized face-match is the first step for follow-up investigations involving showing potential matches to witnesses, searching fingerprint databases, and seeking DNA matches. The FBI's description of its enrolled database states:

"Candidate photos returned to the law enforcement agency are provided as investigative leads only and are not positive identification. Although facial recognition technology has become increasingly accurate, authorized users of the NGI-IPS are prohibited from relying solely on the candidate photos to conduct law enforcement action."[39]

The following Sections explain how law enforcement uses of computerized face-matching work in traditional investigative settings.

About a fourth of the law enforcement agencies in the United States use face-recognition technology.[40] A 2019 law enforcement foundation study of face-recognition technology identified nineteen different uses, generally falling into three categories:

---

39. Erin M. Prest, *Privacy Impact Assessment: NGI-Interstate Photo System,* FBI 2 (Oct. 29 2019), https://www.fbi.gov/file-repository/pia-ngi-interstate-photo-system.pdf/view [https://perma.cc/NV6A-N4CJ] (describing system that includes 38 million photographs for use by law enforcement face-recognition systems).

40. Jillian Slaight & Ryan LeCloux, 3 WIS. POL'Y PROJ., no. 4, Mar. 2020, at 1, 4–5, https://docs.legis.wisconsin.gov/misc/lrb/wisconsin_policy_project/facial_recognition_privacy_3_4.pdf [https://perma.cc/8KA7-Z2ML].

- field use
- investigative use[41]
- custodial and supervisory use[42]

Specifically, the nineteen uses include: (a) narrowing the field of suspects down to a manageable number; (b) exonerating the falsely accused; (c) identifying the mentally ill; (d) helping return children to their parents; and (e) determining the identity of deceased persons.[43] Such applications of the technology involve different permutations of matching.

A. *Permutations*

Distinguishing the permutations of types of matching is useful in classifying law enforcement uses of computerized face-matching as well as relating those uses to the capabilities and limitations of the technology.[44] The following permutations exist:

One unknown to many knowns (1U: nK). This is the permutation used to identify an unknown suspect when his image is available from surveillance video or an on-scene snapshot.

One known to many knowns (1K: nK). This permutation would be useful in identifying an imposter. If the goal is to verify the identity of the known person, one should use the one-known to one-known permutation.

---

41. The IJIS catalog emphasizes these applications:

> - matching surveillance photos with entries in a correctional mugshot database to identify suspects in a $5,000 Home Depot theft.
> - matching online profiles against DMV photos to identify suspects for a sexual assault.
> - apprehending a fugitive by comparing a photo of the suspect in disguise and comparing it with entries in a booking photo database containing more than 4 million images.
> - Identifying a suspect in a theft during a date by comparing a candid shot on a cellphone with a statewide mugshot database.

IJIS INSTITUTE AND IACP LAW ENFORCEMENT IMAGING TECHNOLOGY TASK FORCE, LAW ENFORCEMENT FACIAL RECOGNITION USE CASE CATALOG 11–15 (2019), https://www.ijis.org/resource/collection/93F7DF36-8973-4B78-A190-0E786D87F74F/Law_Enforcement_Facial_Recognition_Use_Case_Catalog.pdf.

42. *Id.* at 15.

43. *Id.* at 7.

44. *See generally id*. at 4 (distinguishing *identification*, one-to-one analysis, from *discovery*, one to many analysis).

Many unknowns to one known (nU: 1K). This permutation would be useful in scanning a stream or a crowd of persons for a known person—a fugitive, a suspect, or an intelligence target.

Many unknowns to many unknowns (nU: nU). This permutation applies if the user is scanning a stream or a crowd of persons for the presence of anyone who may be a suspect, or an intelligence target, because of the frequency with which she appears, without having anyone, in particular, in mind. This permutation is also useful in a database management context, in which two databases are being joined and the user wants to include only those records that are different between the two. The content of the images does not matter, only whether they are different.

Many knowns to one known (nK: 1K). This permutation is useful in a housekeeping function to determine whether a new image is already present in a database. The same utility exists for the reciprocal, one known to many knowns.

One known to one known (1K: 1K). This is the permutation useful for verifying the identity of someone who claims to be someone, as at a checkpoint or registration desk.

One unknown to many unknowns (1U: nU). This permutation has fewer obvious uses. It might be helpful for an intelligence agency seeking to determine leadership at mass demonstrations, or for an anti-gang unit of a law enforcement agency to determine gang leadership. If the same face shows up in imagery of every event, it is likely possible that the owner of the face has a leadership position.[45]

B. *Narrowing the Class of Suspects*

Any criminal investigation must define a class of suspects. In some cases, the task will be easy: the perpetrator is caught in the act or is still on the scene with witnesses around. In other cases, the perpetrator has fled, and the police must talk to witnesses and perform various kinds of crime-scene forensic analysis to determine who might have committed the crime. When surveillance imagery is available, face-recognition can play a key role in this process. The investigator obtains a probe image from the surveillance recording, and inputs it into an automated face-matching system. The system outputs one or more—usually several—potential matches, assigning probabilities to each. This may result in a match with a single individual with high reliability. That may be enough

45. The difference between this permutation and the nU: nU permutation is that, in the 1U: nU scenario, a specific candidate already has been identified.

to establish probable cause for arrest[46] and eventually to obtain a conviction. In other cases, however, the program indicates reasonably close matches with several faces. That is not enough, by itself, to establish probable cause to believe that any one of them committed the crime. It is, however, a useful step forward in the investigation: investigators can focus their attention on only a handful of individuals and use conventional techniques to figure out which one of them is responsible.[47]

Most law enforcement agencies do not consider a positive match from current face-recognition technology to constitute admissible evidence. Instead, they use the computerized matches as an "investigative lead" for additional investigative steps. Presenting the results to witnesses is considered in the next Subsection. The enrolled database has metadata associated with each photograph, which usually includes a name, address, age, known occupations, and criminal history. The investigator can rule out some of the potential face-matches based on their location, and other circumstances, such as incarceration at the time of the crime. If the crime occurred in the tidewater region of Virginia, in Lancaster County, someone who is known not to venture far from a lifelong home in the far western part of the state, near Lee County, is an unlikely suspect. Types of crimes involved, derived in from suspects' criminal histories, also may also be useful.

C. *Supplementing Eyewitness Identification*

When witnesses exist, information from them is valuable in narrowing the search further. If the witness says that the perpetrator was a young black male, seventy-year-old white females can be excluded from the computer-generated photo array.[48]

Then, computer-generated potential matches can be included in a lineup, or if the witness is shown only the top match, in a show up.[49]

---

46. *But see* Douglas A. Fretty, *Face-Recognition Surveillance: A Moment of Truth for Fourth Amendment Rights In Public Places*, 16 VA. J.L. & TECH. 430, 458 (2011) (arguing that face-matching algorithm with substantial failure rate cannot give rise to probable cause for detection or search).

47. Interview with Zachary Beaver, Esq., former Indiana State Police Sergeant (June 10, 2020) (describing use of Indiana State Police face-recognition capability).

48. The reliability of the computerized face-matching system would be questionable, of course, if it selects a seventy-year-old white female as a potential match for a young black male.

49. A show up is the appearance of an individual before a witness in the field, as when police officers arrest a suspect and bring her to a witness to see if the witness can identify her. Clare Garvie, *Garbage In, Garbage Out: Face Recognition on Flawed Data*, GEO. L. CTR. ON PRIV. & TECH. (May 16, 2019), https://www.flawedfacedata.com/ [https://perma.cc/8A39-45FU]; State v Henderson, 27 A.3d 872, 902–03 (N.J. 2011) ("Showups are essentially single-person lineups: a single suspect is presented to a witness to make an identification. Showups often occur at the scene of a crime soon after its commission."); People v. Sammons, 949 N.W.2d 36, 80 n.1

Either lineup or show up can be accomplished by presenting the computer-generated images to the witnesses, or the subjects of the suggested matches can be rounded up physically (if they can be found and induced to cooperate) and presented in conventional face-to-face fashion. If a witness picks the defendant out of a computer-generated array of faces, there is no reason that the analysis legally should be any different from that applied to conventional lineups.

Suggestiveness is a potential issue in these computer-generated lineups and show ups, just as it is in their conventional equivalents.[50] If a witness is shown only one computer-selected image, the witness's corroboration may be so closely tied to the computerized face-recognition match that it lacks independence.[51]

In some cases, the police may be motivated to commission an artist's sketch of a suspect's face based on a combination of surveillance imagery and witness descriptions. The sketch might then be used as a probe image against an enrolled database. Reliability of the computerized match would depend on: (a) the resolution of the surveillance image; (b) the accuracy of the witness descriptions; (c) the accuracy of the artist's rendition; and (d) the robustness of the matching algorithms.

D. *Corroboration by Other Forensic Techniques*

Once a computerized face-match has identified someone as a person of interest, that person's fingerprints can then be compared to a fingerprint database. The same thing can be done with DNA—if probable cause exists to obtain the DNA. A match of either the fingerprints or the DNA corresponding to the face-match would be strongly corroborative.

E. *Field Identification*

In some cases, the police may detain a subject who refuses to identify himself or who provides an identification that the police suspect is false. Face-recognition technology can be useful in this setting because it enables the police to verify the subject's identity. This would involve one-known to one-known matching.

The IJIS Catalog provides examples of useful one-to-one matching: *matching an unknown face with one other face*. This might be the case, for example, if a suspect claims she is not the person shown in a

---

(Mich. 2020) (quoting *Showup*, BLACK'S LAW DICTIONARY (11th ed. 2019)) ("A showup is '[a] police procedure in which a suspect is shown singly to a witness for identification.'").

50. *See* discussion *infra* Section IV.E (analyzing caselaw on suggestiveness of lineups and show ups). Manson v. Braithwaite, 432 U.S. 118, 132–33 (1967) (Marshall, J., dissenting) (arguing that corporeal lineups are more reliable than photograph arrays and that any method is more reliable if it presents multiple subjects rather than only one).

51. *Sammons*, 949 N.W.2d at 44–46 (extensively criticizing show ups as inherently suggestive, although not banning them altogether).

surveillance video. Face-recognition techniques can be applied both to the surveillance image and a newly created image of the suspect. In some cases, this has proven useful in situations where a perpetrator has worn a disguise or concealed her identity in other ways. Of course, the utility of this application requires reasonably good images for comparison. If the surveillance photos show someone wearing a facemask, a later, clean facial image of the suspect will be of little use.

Verification of identity is another one-to-one application. It is useful wherever a legitimate need exists to confirm that someone is who she says she is, for example passport control at national borders or for facility entry. No database is required for this application, simply two images: one taken at the time of registration, such as a driver's license, and the other taken at the moment of identification. This obviously involves one-to-one matching. It is used to activate iPhone 10 and above.[52]

The police might also use the subject's photograph as a probe image against an enrolled database, in one-unknown to many-knowns matching, to see if the subject is perhaps wanted on outstanding warrants or parole violations. This might occur as part of traffic stops, for example. An officer taking a driver's license to do a quick check can use the photograph on the driver's license as a probe image and run it against various enrolled databases. He could then match the known to unknowns for crimes without a suspect. This could be especially useful for incidents committed by out-of-state perpetrators with out-of-state licenses—but only if the officer has access to out-of-state enrolled databases.

Another example of one-to-many matching is an *effort to identify a subject* outside the criminal prosecution context, for example, a disabled person found wandering, a lost child, or a corpse. Similarly, in the context of an arrestee or other person of interest, who refuses to give his name or to provide any other information, face-recognition can be used to establish identity.

F. *Booking Arrestees*

One of the purposes of the post-arrest booking process is to determine if the arrestee is wanted for crimes other than the one for which he was arrested. Face-recognition can become a regular part of the booking process for arrestees. After an arrestee's mug shot is taken, that photograph can be used as a probe photo against a many-known enrolled

52. Glenn Fleishman, *Face ID on the iPhone X: Everything You Need to Know About Apple's Facial Recognition*, MACWORLD (Dec. 25, 2017), https://www.macworld.com/article/3225406/face-id-iphone-x-faq.html [https://perma.cc/8DAY-7EK9] (describing how users unlock the iPhone 10).

databases. If a possible match occurs, it can easily be confirmed with fingerprints, and, if doubt still exists, with DNA.[53]

The same process could be used for traffic and other "Terry" stops,[54] if face-recognition systems are fast enough that the "stop" does not turn into an "arrest."[55] In this way, face-recognition software would supplement the usual "wants and warrants" radio check.[56]

G. *Scanning Crowds to Find Fugitives*

Real-time face surveillance involves scanning crowds or streams of unknown people, looking for matches with fugitives, suspects, or intelligence targets. This is the most expansive use of face-recognition technology and of many-to-many matching. It involves scanning the faces of everyone in a crowd or stream of individuals, with each face being compared with those in the database. This might be used, for example, to detect fugitives or undocumented migrants. The technical limitations on this kind of use relate mainly to the speed of processing. If the application must process faces present in long lines at a security checkpoint, a face-recognition application that takes significant time for each face is unacceptable. Over time, however, the technology will get faster, and this application will become more feasible. Commentators have expressed concern with police body cameras' ability to acquire images of random faces,[57] and use of the technology at the 2001 Super Bowl.[58]

A modification of this application involves scanning not every face in a crowd or line, but only certain faces that have some indication warranting interest.

---

53. All inmates in Indiana are required to have a picture and fingerprints taken, and all violent crimes and felonies require a DNA sample. Beaver, *supra* note 26.

54. *See* Terry v. Ohio, 392 U.S. 1, 20–22 (1968) (holding that an investigatory "stop and frisk" is a Fourth Amendment seizure and search but does not require the probable cause necessary for an arrest; specific and articulable facts giving rise to reasonable suspicion suffice).

55. *See* Rodriguez v. United States, 575 U.S. 348, 358 (2015) (analyzing whether extending a Terry stop by seven or eight minutes to allow time for a dog sniff violated the Fourth Amendment, unless reasonable suspicion of other criminal activity existed); *id.* at 350 (quoting Illinois v. Caballes, 543 U.S. 405, 407 (2005)) ("A seizure justified only by a police-observed traffic violation, therefore, 'become[s] unlawful if it is prolonged beyond the time reasonably required to complete th[e] mission' of issuing a ticket for the violation.").

56. *See* United States v. Martinez-Cortes, 566 F.3d 767, 771 (8th Cir. 2009) (approving detention long enough to do wants and warrants check).

57. Katelyn Ringrose, *Law Enforcement's Pairing of Facial Recognition Technology with Body-Worn Cameras Escalates Privacy Concerns*, 105 VA. L. REV. ONLINE 57, 58 (2019) (describing risk of general scanning of faces by police officers wearing body cameras).

58. Alexander T. Nguyen, *Here's Looking at You, Kid: Has Face-Recognition Technology Completely Outflanked the Fourth Amendment?*, 7 VA. J.L. & TECH. 2, *1 (2002) (describing use of face-recognition system to scan 100,000 ticketholders at the 2001 Super Bowl).

H. *Artist Reconstructions*

Sometimes artist reconstructions based on witness descriptions are used as the probe photos.[59] Compusketch is a commercial program, available since 1987, that creates face sketches from witness interviews. It is faster than a human artist and does not require a high level of skill in the user.[60] A police department might interview a witness to create a Compusketch image and use it as the probe image in a face-recognition system.

When an artist reconstruction is used as a probe image for a face-recognition system, testing the reliability of any resulting face-match requires testing the reliability of the sketch, whether made by a human artist or by a sketching computer program. The question is: how faithfully does the sketch represent the description given by a human witness? The reliability of the description is a separate question.

I. *Law Enforcement Products in the Marketplace*

Several commercial face-recognition products are marketed to law enforcement agencies and make the following claims:

- NEC Corp. is a Japanese corporation that advertises, "NEC's technology can match a subject's face from images with resolutions as low as 24 pixels, even if the subject is on the move, or the face partially concealed by hats, scarves or glasses, or head angle. It also facilitates video surveillance in crowded, poorly lit areas at unmatched speed and volume in real time."[61]

- Idemia advertises:

> Face Expert enables trained forensic investigators, analysts, and detectives to solve crimes thanks to automatic face finding and tracking of photos or videos. Faces from images or videos can be matched against a database to identify a wanted or missing person. Once facial images are matched, analysts can link a suspect to a crime. The application provides the ability to navigate within the database to capitalize on information from

59. *See* Garvie, *supra* note 49; Klum, *supra* note 17.

60. *See* R. Bocklet, *Suspect Sketches Computerized for Faster Identification*, 35 LAW & ORDER, no. 8, Aug. 1987, at 61.

61. *Face Recognition*, NEC, https://www.nec.com/en/global/solutions/biometrics/face/index.html [https://perma.cc/W47X-V7A3] (last visited Jan. 7, 2021).

> previous searches. It can also help match recently booked offenders with unsolved cases. Easy to use and powerful, the system enables users to deal with cases using still images, videos, and difficult to process images. Its 3D modeling tool reconstructs a facial image from multiple partial views, while the image processing enhances poor quality pictures and non-frontal views.[62]

Idemia reports that it scored well on NIST tests and is the "leading" provider of law enforcement solutions in the United States.[63]

- Facefirst advertises "instant identification, smarter patrols, and safer streets."[64] It offers "mobile face-recognition," and reassures potential users that "face-recognition doesn't profile." Use of it "minimize[s] lawyers and negative press."[65]
- Rank One Computing[66] advertises face-recognition algorithms for law enforcement, refined to eliminate demographic bias. Its chief engineer, Scott Klum, has authored several academic papers on use of face-recognition algorithms.[67] Its algorithms were used in the program featured in the New York Times misidentification story reviewed in SectionVI.B.
- Vigilant Solutions Facesearch,[68] offers, "Images and analytics power investigations."

---

62. *Face Expert*, IDEMIA, https://www.idemia.com/face-expert [https://perma.cc/3ZD6-JN3B] (last visited Jan. 7, 2021).

63. *Idemia Facial Recognition Algorithm Outperforms Other U.S. Government Agency Providers at Recent NIST Test*, IDEMIA (Mar. 26, 2019), https://www.idemia.com/press-release/idemia-facial-recognition-algorithm-outperforms-other-us-government-agency-providers-recent-nist-test-2019-03-26 [https://perma.cc/5XDJ-HAC3].

64. *How to Calculate Face Recognition ROI for Law Enforcement*, FACEFIRST, https://www.facefirst.com/blog/face-recognition-roi-law-enforcement [https://perma.cc/PK2X-2832] (last visited Jan. 7, 2021).

65. *What is the True Cost of a False Arrest for Law Enforcement Officials?*, FACEFIRST, https://www.facefirst.com/blog/law-enforcement-cost-false-arrest-far-just-bad-press/ [https://perma.cc/UNH3-AKEX] (last visited Jan. 7, 2021).

66. *Company* Overview, RANK ONE COMPUTING, https://www.rankone.io/company/ [https://perma.cc/ZB9B-LF8F] (last visited Jan. 7, 2021).

67. *Id.*; *see* Klum, *supra* note 17; Klare et al., *supra* note 13.

68. *Vigilant FaceSearch Identity Matching and Verification*, MOTOROLA SOLUTIONS https://www.motorolasolutions.com/en_us/products/command-center-software/analysis-and-

- Animetrics advertises software algorithms that allow law enforcement agencies to enhance probe photos incident to submitting them to databases.[69]
- Clearview AI[70] has stirred up the most controversy. It matches photographs taken on the spot against 3 billion images from Facebook, YouTube, Venmo, and other websites.[71]

BuzzFeed reported on use of Clearview by Illinois law enforcement:

> In Illinois, most of the more than 105 entities that used Clearview were local police departments. The two departments with the most searches, according to company data reviewed by BuzzFeed News, were the Macon County Sheriff's Office, which had run nearly 2,000 searches as of late February, and the Naperville Police Department, which had scanned nearly 1,700 photos. . . . Several federal agencies' field offices in the state, including the Chicago offices of the FBI and the Bureau of Alcohol, Tobacco, Firearms and Explosives, also used Clearview, according to data seen by BuzzFeed News.[72]

In *Mutnick v. Clearview AI, Inc.*,[73] David Mutnick sued, on behalf of a class, for an injunction against Clearview AI, arguing that its use violated the Illinois Biometric Information Privacy Act (BIPA).[74] Clearview AI moved to dismiss the action as moot, after it cancelled all its contracts with anyone except law enforcement agencies and stopped using the system altogether in Illinois.[75]

---

investigations/vigilant-facesearch-facial-recognition-system.html [https://perma.cc/V5RJ-6E6P] (last visited Jan. 7, 2021).

69. *ForensicaGPS*, ANIMETRICS, http://animetrics.com/?content=products/forensicaGPS [https://perma.cc/ML8R-TBXM] (last visited Jan. 7, 2021).

70. CLEARVIEW.AI, https://clearview.ai/ [https://perma.cc/7TY4-6BZ9] (last visited Jan. 7, 2021) (advertising "Available now for Law Enforcement").

71. Kashmir Hill, *The Secretive Company that Might End Privacy as We Know It*, N.Y. TIMES (Feb. 10, 2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html [https://perma.cc/ZA6A-ZNXF] (describing Clearview AI).

72. Ryan Mac, et al., *Clearview AI Has Promised To Cancel All Relationships With Private Companies*, BUZZFEEDNEWS (May 7, 2020, 6:50 PM), https://www.buzzfeednews.com/article/ryanmac/clearview-ai-no-facial-recognition-private-companies [https://perma.cc/Q4XQ-7X5K].

73. No. 20-cv-512, 2020 WL 4676667 (N.D. Ill. Aug. 12, 2020).

74. 740 ILL. COMP. STAT. ANN. 14/1 (LexisNexis 2020).

75. Defendants' Memorandum of Law, *Mutnick*, 2020 WL 6131216 (May 6, 2020) (No. 20-cv-512) (opposing injunction and arguing that case is moot because of change in business practices to omit private entities as customers and to omit data on Illinois residents); Nick Statt, *Clearview AI to Stop Selling Controversial Facial Recognition App to Private Companies*, THE

Presumably, this represented an economic decision by Clearview AI that it was better off continuing to earn revenue from law enforcement uses outside Illinois rather than to risk a shutdown of its operation altogether. The case remains pending awaiting action on the defendant's motion to dismiss. Facebook settled another class action under the same statute for $550 million earlier in 2020.[76]

Many developmental tools using the popular programming language, Python, are available on the Web.[77] This would enable more sophisticated agencies to develop their own computerized face-matching systems, using third party components, including training databases.

IV. LEGAL ANALYSIS

The analytical framework for assessing the legality of computerized face-recognition in criminal prosecutions involves the following possibilities:

- The law may limit collection of images of faces by law enforcement agencies;[78]
- The law may limit the use of matches resulting from her computer comparison of facial images; [79]
- The law may limit law enforcement agencies' use of computer software to match faces; [80]
- The law may limit the use of a computerized matches as evidence at trial because it violates the Confrontation Clause; [81]

VERGE (May 7, 2020, 8:29 PM), https://www.theverge.com/2020/5/7/21251387/clearview-ai-law-enforcement-police-facial-recognition-illinois-privacy-law.

76. Jay Peters, *Facebook to Pay $550 Million to Settle Privacy Lawsuit over Facial Recognition Tech*, THE VERGE, (Jan. 29, 2020, 7:17 PM), https://www.theverge.com/2020/1/29/21114358/facebook-550-million-settle-lawsuit-facial-recognition-technology-illinois [https://perma.cc/DH4Z-QR4A]. Section IV.C, *infra*, analyzes the Illinois statute and the Facebook case.

77. *See* Adrian Rosebrock, *Face Recognition with OpenCV, Python, and Deep Learning*, PYIMAGESEARCH (June 18, 2018), https://www.pyimagesearch.com/2018/06/18/face-recognition-with-opencv-python-and-deep-learning/ [https://perma.cc/M5KG-6EUR] (providing tutorial and executable Python modules for face recognition).

78. *See infra* Section IV.D.4.

79. *See infra* Section IV.F.4.

80. *See infra* Section IV.C.

81. *See infra* Section IV.D.1.

- The law may limit use of computerized face-matches as evidence at trial because such evidence is inadmissible hearsay; [82]
- The law may limit the use of computerized face-matches as evidence at trial because it violates the Fourth Amendment or broader privacy interests; [83]
- The law may limit the use of computerized face-matches as evidence at trial because its probative value is outweighed by its prejudicial effect; [84] and
- The law may limit the use of a computerized face-match evidence at trial because the process producing such matches is unreliable.[85]

Each of these possibilities depends upon the interplay of common law rights to privacy and against trespass, federal and state statutes focused on privacy—or on face-recognition software more specifically, on the rules of evidence, and on the Fourth and Sixth Amendments to the United States Constitution and their counterparts in state constitutions.

The law of face-recognition in criminal procedure is still being crystallized. A much broader debate about the appropriate role of biometric identification techniques in a free society has implications for and has motivated some proposals for statutory restrictions on police use. But these have been reduced to statutory form in only a few places. Evaluating commentators' proposals should depend on a careful assessment of how computerized face-recognition implicates privacy interests.

Caselaw addressing computerize face-recognition in criminal prosecutions is sparse, unlike the more robust caselaw addressing the techniques in the commercial context.

Pertinent caselaw from analogous identification techniques is abundant, however, and one can synthesize from this body of law basic principles to be applied to face-recognition. Fingerprint matches and, more recently, DNA matches are regularly used in criminal investigations and prosecutions. The touchstones for validating their reliability and justifying reliance on them can be adapted to computerized face-recognition.

The following Subsections begin by summarizing the caselaw and commentary on computerized face-recognition. Then they move to probe the claim that computerized face-recognition in the criminal justice

82. *See infra* Section IV.D.1.
83. *See infra* Section IV.D.4.
84. *See infra* Section IV.D.3.
85. *See infra* Section IV.E.1.

context infringes personal privacy interests, the hallmark of Fourth Amendment analysis, including its exclusionary rule for violations.

Then, the Section evaluates federal and state statutes, following by application of Sixth Amendment Confrontation Clause law to computerized face-recognition, and follows that analysis by its Fourth Amendment counterpart. Finally, the Section analyzes the abundant caselaw on other forms of identification based on appearance and physical artifacts to synthesize some touchstones to judge whether computerized face-matching has sufficient reliability to support a conviction.

A. *Caselaw and Commentary*

Caselaw on the use of computerized face-recognition evidence in criminal cases is sparse. In *Blane v. Division of Motor Vehicles*,[86] the Delaware common pleas court rejected an appeal from a driver's license suspension. The court approved use of primitive face-recognition software to determine that the appellant had fraudulently applied for a driver's license by pretending to be someone else.[87]

United States v. Gibson[88] rejected a speedy trial claim by a defendant who was arrested almost 15 years after he was indicted, based on face-recognition technology applied to a driver's license and passport application.[89]

In another case, *Hutcherson v. State*,[90] the court expressed doubt about the reliability of the technology. The Arkansas supreme court denied a habeas corpus petition by an inmate seeking application of face-recognition technology to a video recording, which, he claimed, would show that he was not the perpetrator of an armed robbery.

> While appellant refers to advances in facial-recognition technology, he does not demonstrate that the new technology is accepted in this state or that it is substantially more probative than that available at the time of trial, that the videotape is available with an unbroken chain-of-custody, or that the tape reveals facial features capable of being enhanced through the application of a particular technology. In short, he has not established that there is new technology

86. No. CPU5-10-001253, 2011 WL 13175124 (Del. C.P. June 30, 2011).

87. *Id.* at *3–*4; *accord*, United States v. Badiane, 725 Fed. App. 828, 831–35 (11th Cir. 2018) (allowing testimony of past passport fraud, based on face-recognition software).

88. No. 8:00-cr-442-T-27AEP, 2016 WL 845272 (M.D. Fla. Mar. 4, 2016).

89. *Id.* at *2.

90. 2014 Ark. 326, 438 S.W.3d 909.

> that would exclude him as the perpetrator of the robbery of the Texaco station.[91]

Law-review[92] and popular-press and media commentary,[93] on the other hand, is abundant, and mostly negative.

B. *Privacy Concerns: Separating the Wheat from the Chaff*

The upwelling alarm about data privacy focuses on any capture of

---

91. *Hutcherson*, 438 S.W.3d at 913.

92. *E.g.*, Blake A. Klinkner, *Facial Recognition Technology, Biometric Identifiers, and Standing to Litigate Invasions of Digital Privacy*, 42 WYO. LAW. 44 (2019); Mark Lanterman, *Facial Recognition Technology Brings Security & Privacy Concerns*, 74 BENCH & B. MINN. 12 (2017); John Nawara, *Machine Learning: Face Recognition Technology Evidence in Criminal Trials*, 49 U. LOUISVILLE L. REV. 601 (2011); Fretty, *supra* note 46; Nguyen, *supra* note 58; Kevin Davis, *Face Time*, 103-Oct A.B.A. J. 16 (2017); Robert H. Thornburg, *Face Recognition Technology: The Potential Orwellian Implications and Constitutionality of Current Uses Under the Fourth Amendment*, 20 J. MARSHALL J. COMPUT. & INFO. L. 321 (2002); Claudia Cuador, *From Street Photography to Face Recognition: Distinguishing Between the Right to Be Seen and the Right to Be Recognized*, 41 NOVA L. REV. 237 (2017); Bridget Mallon, *Every Breath You Take, Every Move You Make, I'll Be Watching You: The Use of Face Recognition Technology*, 48 VILL. L. REV. 955 (2003); Mohammed Osman & Edward Imwinkelried, *Facial Recognition Systems*, 50-3 CRIM. L. BULL. Art. 11 (2014); Christopher W. Savage., *Washington Enacts First-In-Nation State Law Regulating Governmental Use of Facial Recognition*, 32 INTELL. PROP. & TECH. L.J. 21 (2020); Elias Wright, *The Future of Facial Recognition Is Not Fully Known: Developing Privacy and Security Regulatory Mechanisms for Facial Recognition in the Retail Sector*, 29 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 611 (2019).

93. *E.g.*, Kashmir Hill, *Wrongfully Accused by an Algorithm*, N.Y. TIMES (June 24, 2020), https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html [https://perma.cc/YSL3-QJF7]; Karen Weise & Natasha Singer, *Amazon Pauses Police Use of Its Facial Recognition Software*, N.Y. TIMES (June 10, 2020), https://www.nytimes.com/2020/06/10/technology/amazon-facial-recognition-backlash.html [https://perma.cc/8MZF-DP5R]; Shira Ovide, *A Case for Banning Facial Recognition*, N.Y. TIMES (June 10, 2020), https://www.nytimes.com/2020/06/09/technology/facial-recognition-software.html [https://perma.cc/4UPJ-EP48]; Davey Alba, *A.C.L.U. Accuses Clearview AI of Privacy 'Nightmare Scenario,'* N.Y. TIMES, May 20, 2020, at B3; Julia Horowitz, *Tech Companies Are Still Helping Police Scan Your Face*, CNN (July 3, 2020, 8:36 AM), https://www.cnn.com/2020/07/03/tech/facial-recognition-police/index.html [https://perma.cc/69T6-9RZU]; Brian Fung, *Democratic Lawmakers Propose Nationwide Facial Recognition Ban*, CNN (June 25, 2020, 1:37 PM), https://www.cnn.com/2020/06/25/tech/facial-recognition-legislation-markey/index.html [https://perma.cc/M3WH-2PTN]; Clare Duffy, *Microsoft President Calls for Federal Regulation of Facial Recognition Technology*, CNN (June 18, 2020, 6:05 PM), https://www.cnn.com/2020/06/18/tech/brad-smith-microsoft-facial-recognition/index.html [https://perma.cc/E9JG-VPZD]; Brian Fung, *Tech Companies Push for Nationwide Facial Recognition Law. Now Comes the Hard Part*, CNN (June 13, 2020, 1:06 PM), https://www.cnn.com/2020/06/13/tech/facial-recognition-policy/index.html [https://perma.cc/EQ8C-FK5T]; Brian Fung, *Microsoft Says It Won't Sell Facial Recognition Technology to U.S. Police Departments*, CNN (June 11, 2020, 2:13 PM), https://www.cnn.com/2020/06/11/tech/microsoft-facial-recognition-police/index.html [https://perma.cc/KUZ2-F8Z4].

personally identifiable information and any use of it.[94] Much of the opprobrium directed at Facebook seems motivated by the ubiquity and quality of its face-matching. Publicly expressed concerns extend to law enforcement uses that pose no more of a privacy threat than fingerprints or DNA matching; yet fingerprints and DNA are regular features of the criminal justice system. Indeed, some states have enacted statutes that limit or prohibit use of face-matching by law enforcement.[95]

Figuring out where face-recognition fits in the law should begin with an assessment of the particular risks to privacy that the different applications present, followed by an evaluation of prescriptions already adopted for other personally identifying data such as fingerprints and DNA. Then, those privacy risks should be balanced against public benefits from use of particular technologies. It is not clear to this author how public welfare is served by allowing a robber to go undetected or a fugitive to remain at large. The legitimate concern is prosecution of the wrong subject and face-recognition reduces the chances of that.

Working through the application typology developed in Section III, one can see privacy concerns are attenuated or nonexistent with respect to many of the applications, and that they are likely outweighed by law enforcement interests in most of the other applications.

Verification of identity is an easy case. The subject has voluntarily allowed his photograph to be taken when he got his driver's license or applied for a passport, and he is voluntarily allowing his image to be recorded again at the point where he presents himself to verify his identity. Some take the position that one should not constantly have to identify himself as he moves about in a free society. The author, for example, resents having to present a photo ID when he checks into a hotel. But the invasion of privacy occurs, not because of the face-recognition technology, but because of the identification requirement itself. If the invasion is greater than should be tolerated in a free society, the identification requirement should be eliminated, not the particular technology used for it, as many voting rights advocates argue.[96]

A different set of considerations arises with applications intended to identify an unknown person who is present, as with a disabled person, a child, a corpse, or someone who has been detained by law enforcement officers and refuses to identify himself. When the lack of identification is

---

94. *See* Brian Fung, *The Unlikely Activist Behind the Nation's Toughest Privacy Law Isn't Done Yet*, CNN (Oct. 10, 2019, 10:12 AM), https://www.cnn.com/2019/10/10/tech/alastair-mactaggart/index.html [https://perma.cc/GG24-AX5N] (reporting on crusade of California privacy activist Alastair Mactaggart).

95. *See* KELSEY Y. SANTAMARIA, CONG. RSCH. SERV., R46541, FACIAL RECOGNITION TECHNOLOGY AND LAW ENFORCEMENT: SELECT CONSTITUTIONAL CONSIDERATIONS (2020) (finding states have regulated law enforcement's use of facial recognition technology).

96. *See* ACLU, *Oppose Voter ID Legislation - Fact Sheet* (May 2017), https://www.aclu.org/other/oppose-voter-id-legislation-fact-sheet [https://perma.cc/LH7H-NS9U].

the result of unwillingness, the target has unambiguously asserted a privacy interest. Identifying him nevertheless invades that interest. Whether the law should allow the invasion involves competing interests no different from those involved in any law enforcement stop: whenever an agent of law enforcement stops someone and asks for identification, or goes further and takes fingerprints or a DNA sample. There is no reason that the law enforcement privilege of matching a face when the target is a suspect, should be different from the privilege to demand a driver's license, fingerprints, or DNA. The interest of a perpetrator in not being identified is clear. So, on the other hand, is the public interest.

The law requiring reasonable suspicion for law enforcement stops and requiring probable cause for arrests is highly developed, the intrusion on liberty interests resulting from accurate identification of faces does not seem to be significantly greater than the deprivation occasioned by the stop or the arrest itself.

The greatest and most legitimate privacy concerns arise from the many applications for crowd searching. When such applications are fully deployed, it will no longer be possible to hide in a crowd. That will be the last straw in eliminating anonymity that is available in urban society, and which has been available, in some fashion, for centuries. In the 19th century, if one developed an unsavory reputation—even to the point of having outstanding arrest warrants—one could go West and easily establish a new identity without much fear of being discovered. With current technology, however, the time required to do computerized face-matching for a crowd or stream of people passing a checkpoint[97] is likely to deter its routine use.

This analysis suggests that the core concept of legal limitations on face-recognition might center on the core concept of limitations on electronic surveillance. For wiretaps and access to stored records alike, law enforcement agents must identify a particular target and justify their interest in him. It is certainly not permissible under the Fourth Amendment simply to listen in on every voice communication or to read every email. Even the NSA's notorious Stellar Wind does not do this; it analyzes traffic patterns, not content.

Fingerprint and DNA technologies limit privacy because they make it difficult for someone to start over with a new identity—a common practice in the Old West. Frustrating that goal of anonymity or pseudonymity, however, depends on the availability of cost-effective one-unknown to many-known matching, which has been possible with both types of biometric information only for a little more than a decade.

---

97. *See* discussion *supra* Section II.D (explaining how to calculate face-matching processing speeds).

Face-matching technology limits privacy by making it impossible for someone to hide in a crowd. Frustration of that privacy interest likewise depends upon the efficacy of one-unknown to many-known matching.

Privacy interests have only an attenuated relationship to Confrontation Clause analysis. A potential witness whom the defense claims right to confront has a privacy interest in not being bothered or compelled to reveal information. Privacy, however, is at the core of a Fourth Amendment analysis, after *United States v. Katz*.[98]

C. *Federal and State Statutes*

Currently, no federal statutes limit law enforcement the use of face-recognition.[99] Several states and municipalities restrict the use of face-recognition technology by the private sector[100] and, less often, law enforcement agencies.[101] Proposed legislation is springing up all over the place.[102]

Washington S.B. 6280[103] is a paradigm of a statute directly addressing face-matching by law enforcement. It regulates the use of face-recognition technology by state and local government. The statute requires that uses of face-recognition computer software be reported to the legislative body with jurisdiction over the agency user.[104] This reporting presumably occurs once, before the product is used at all, and not for each match.

Once notification is given the user-agency must prepare an "accountability report", including the name of the system and its general capabilities;[105] statements about the data inputs and outputs;[106] description of proposed use of the system, including what decisions are associated with it; and a "clear use and data management policy." The

98. 389 U.S. 347, 353 (1967) (replacing "trespass" analysis with "privacy" analysis for Fourth Amendment search-and-seizure law).

99. *But see* Ringrose, *supra* note 57, at 64–65 (speculative and summary suggestion that federal Video Privacy Protection Act could require compartmentalizing video imagery collected by police body cameras).

100. Slaight & LeCloux, *supra* note 40, at 11–12 (citing various local and state government bans on face-recognition technology).

101. *Id.* at 14 (Criminal Procedure section summarizing state bills that would limit use of face-recognition evidence in criminal trials).

102. *Id.* at 13 (summarizing proposed face-recognition legislation applicable to law enforcement agencies); *see also* Zeb Zankel, *San Francisco Bans Facial Recognition Technology Amidst Wave of Government Scrutiny*, DAVIS WRIGHT TREMAINE LLP: PRIV. & SEC. BLOG (May 23, 2019), https://www.dwt.com/blogs/privacy--security-law-blog/2019/05/san-francisco-bans-facial-recognition [https://perma.cc/ZGQ7-2QJR].

103. 2019 WA S.B. 6280 S.B. 6280, 66th Leg., Reg. Sess. (Wash. 2020).

104. *Id.* at § 3(1).

105. *Id.* at § 2(1).

106. *Id.* at § 3(2)(b)(i).

report must include description of the agency's training procedures,[107] its testing procedures,[108] and information on the rate of false matches and how the agency will address them.[109] The agency must allow public review and comment on the accountability report and update it every two years and submit it to the legislative authority.[110]

An agency using face-recognition software to make decisions with legal effects must "ensure that those decisions are subject to meaningful human review."[111]

It requires vendors to make available an Application Programming Interface (API) that permit tests of "accuracy and unfair performance differences across distinct subpopulations."[112] The API requirement, however, does not require the vendor "to disclose proprietary data."[113]

The statute requires disclosure to criminal defendants of "their use of a facial recognition service on a criminal defendant."[114]

A judge issuing a surveillance warrant must report the facts to the state administrator for the courts.[115]

An agency may not use face-recognition to engage in "ongoing surveillance, conduct real-time or near real-time identification, or start persistent tracking," unless it obtains a warrant, unless exigent circumstances exist, or unless it obtains judicial authorization for limited purposes such as locating or identifying a missing or deceased person.[116]

The statute declares that a single match from a computer system does not constitute probable cause for arrest or warrants.[117] Additionally, agencies may not use face-recognition based on a sketch[118] nor substantively manipulate a probe image.[119]

Elsewhere, more general biometric privacy statutes are being applied to face-recognition. BIPA[120] is one of the most stringent statutes in the country limiting computerized face-recognition. In 2020, Facebook settled a class action lawsuit brought under the statute for $550 million,[121]

107. *Id.* at § 3(d)(vii).
108. *Id.* at § 3(e)
109. *Id.* at § 3(f).
110. *Id.* at § 3(3)–(4).
111. *Id.* at § 4.
112. *Id.* at § 6(1)(a).
113. *Id.* at § (6)(b).
114. *Id.* at § 8.
115. *Id.* at § 8(3).
116. *Id.* at § 11(1).
117. *Id.* at § 11(5).
118. *Id.* at § 11(6).
119. *Id.* at § 11(7).
120. 740 ILL. COMP. STAT. ANN. 14/1 (LexisNexis 2020).
121. Peters, *supra* note 76.

after the United States Court of Appeals for the Ninth Circuit affirmed class certification and standing.[122]

The court described Facebook's face-recognition capability:

> In 2010, Facebook launched a feature called Tag Suggestions. If Tag Suggestions is enabled, Facebook may use facial-recognition technology to analyze whether the user's Facebook friends are in photos uploaded by that user. When a photo is uploaded, the technology scans the photo and detects whether it contains images of faces. If so, the technology extracts the various geometric data points that make a face unique, such as the distance between the eyes, nose, and ears, to create a face signature or map. The technology then compares the face signature to faces in Facebook's database of user face templates (i.e., face signatures that have already been matched to the user's profiles). If there is a match between the face signature and the face template, Facebook may suggest tagging the person in the photo.[123]

The plaintiffs claimed that Facebook violated "sections 15(a) and 15(b) of BIPA by collecting, using, and storing biometric identifiers. . . from their photos without obtaining a written release and without establishing a compliant retention schedule."[124]The court of appeals affirmed the district court's finding of standing,[125] and its certification of the class.[126]

Remarkably enough, one district court concluded that the inclusion of the *victim's* DNA in a law enforcement database violated the Fourth Amendment, because of DNA database restrictions in a state statute.[127]

Paradoxically, Illinois also has a marijuana statute that encourages the use of face-recognition technology.[128] Other states have broadened their privacy statutes to include biometric data, but those statutes do not usually regulate law enforcement agencies.[129]

---

122. Patel v. Facebook, Inc., 932 F.3d 1264, 1277 (9th Cir. 2019).

123. *Id.* at 1268.

124. *Id.*

125. *Id.* at 1274.

126. *Id.* at 1277.

127. *See* United States v. Davis, 657 F. Supp. 2d 630, 665 (D. Md. 2009) (holding that retention of defendant's DNA in database, obtained in a separate case where he was a victim, violated his Fourth Amendment guaranteed privacy interests).

128. Slaight & LeCloux, *supra* note 40, at 11 (discussing Ill. statute requiring face-recognition in marijuana outlets).

129. *See, e.g.*, Stop Hacks & Improve Electronic Data Security Act (SHIELD Act), 2019 N.Y. Laws 117 (2019) (detailing safeguards created to prevent data breaches, though not limiting law enforcement use of face-recognition technology).

D. *Constitutional Limitations*

The Constitution circumscribes the use of computerized face-recognition evidence in two respects, under the Confrontation Clause and under the Fourth Amendment limitations on searches and seizures. The Confrontation Clause comes into play because evidence of a computerized face-match arguably constitutes hearsay, and to admit it violates the Confrontation Clause because it denies the defendant an opportunity to cross examine the originator of the evidence. The Fourth Amendment comes into play because obtaining the image of a suspect's face may be a search.

1. Confrontation Clause

The Sixth Amendment to the United States Constitution guarantees that "[i]n all criminal prosecutions, the accused shall enjoy the right . . . to be confronted with the witnesses against him."[130] This Confrontation Clause guarantee applies to the states.[131] That right has been broadened by the courts to exclude evidence that has not been subjected to cross examination to test its reliability. Thus, as interpreted by the courts, the Confrontation Clause is similar to the common law rule excluding hearsay: an out of court statement offered to prove the truth of the matter asserted therein. Both proceed from the belief that cross examination is the best test of reliability of evidence, and both define their scope in terms of what is an out of court "statement" offered later to "prove the truth of the matter asserted therein." The scope of hearsay exclusions is broader than the scope of confrontational coverage, however. They both apply to out of court statements offered to prove the truth of the matter asserted therein, but the Supreme Court has held that states may prohibit hearsay evidence more broadly than the Confrontation Clause does.[132]

For example, consider the situation where the police interview a witness and the witness says, "I saw the defendant kill the victim." If the police later offer to testify as to the statement, without the witness being present in court, a classic case for exclusion is hearsay is presented. The witness statement was made out of court and is being offered to prove the proposition that the defendant killed the victim. The defendant does not have the opportunity to confront the witness, because she is not in court.

One can apply this example to the computerized face-recognition context. A state police intelligence unit runs a probe image from a surveillance video recording against an enrolled database. The system produces several possible matches. The police take the most probable

130. Crawford v. Washington, 541 U.S. 36, 38 (2004).

131. Pointer v. Texas, 380 U.S. 400, 407–08 (1965).

132. *Crawford*, 541 U.S. at 51 ("[N]ot all hearsay implicates the Sixth Amendment's core concerns."); *id.* at 68–69 (States remain free to adapt hearsay rules.).

match and charge the defendant based on it. What the computerized face-match system "says" is a possible match is an out of court statement. If that match, itself, is offered into evidence, it is being offered to prove the truth of the proposition that the defendant was the perpetrator. So, denying the defendant the opportunity to cross examine the computerized face-matching procedure violates the rule against hearsay and, probably, the Confrontation Clause.

When the witness makes an in-court identification, the Confrontation Clause is not violated, because the witness is available for cross examination. It is only when the identification is made out of court that questions under the Clause arise. In *State v. Allen*,[133] the North Carolina intermediate court held that allowing evidence of an out of court identification based on a photo array violated the Confrontation Clause, but this was a harmless error because of other evidence implicating the defendant.[134]Evidence can escape Confrontation Clause requirements for an opportunity to cross examine when they are not testimonial,[135] or when they are not offered to prove the truth of the matter they assert.[136]

The Supreme Court presented *United States v. Wade*,[137] as a right to counsel case. A criminal defendant has a right to counsel at critical stages of an investigation or prosecution focused on him. The lineup in *Wade* was such a crucial event that also implicated the right to confront. Having counsel at a particular stage affords an opportunity to confront witnesses and other evidence. In *Wade*, the Supreme Court linked the right to counsel at pre-trial proceedings such as lineups with the right to confront.[138] The right to counsel, like the right to confront witnesses, is

---

133. 614 S.E.2d 361 (N.C. Ct. App. 2005).

134. *Id.* at 367.

135. *Crawford*, 541 U.S. at 51–52 (describing Sixth Amendment application to "testimonial" out of court statements; observing that some excludable hearsay statements would not be testimonial).

136. The Confrontation Clause excludes hearsay, which is an out of court statement offered "to prove the truth of the matter asserted" therein. FED. R. EVID. 801(c).

137. 388 U.S. 218, 223–24 (1967).

138. *Id.* at 226–27.

> [T]he principle of *Powell v. Alabama* and succeeding cases requires that we scrutinize any pre-trial confrontation of the accused to determine whether the presence of his counsel is necessary to preserve the defendant's basic right to a fair trial as affected by his right meaningfully to cross examine the witnesses against him and to have effective assistance of counsel at the trial itself. It calls upon us to analyze whether potential substantial prejudice to defendant's rights inheres in the particular confrontation and the ability of counsel to help avoid that prejudice.

Id. at 227.

contained in the Sixth Amendment.[139] Subsequent case law uses *Wade* in the context of confrontation clause controversies as much as right to counsel controversies. Indeed, a "Wade hearing"[140] provides an opportunity to confront pre-trial identification procedures.

But it is not that simple and is not that favorable for the accused. For one thing, there is a substantial body of caselaw that holds that out of court computerized analysis is not subject to the hearsay rule of the confrontation clause, either because it is not a "statement" or because it is not directly used as evidence. Similar treatment of computerize face-matching matches is likely, especially because, under current practice in the current state of technology, it is rare for the prosecution to offer the computer match directly as evidence.[141] Instead, the prosecution uses the computer face-match as a lead to obtain other evidence, including, most prominently, live witness identification in court or through more conventional out of court procedures such as lineups.

Confrontation Clause analysis is muddied by several decisions holding that computer-generated evidence is not hearsay, because it does not involve human intervention. These cases reason that only human adjustments to variables and human-selected options in running computer programs should be subject to cross examination.[142]

This is not the right conclusion. The validity of computer-generated evidence usually depends on the appropriateness of decisions made by the computer programmer. Even a simple spreadsheet summation function may produce the wrong answer if the designer of the spreadsheet has input the wrong equation. In *Melendez-Diaz v. Massachusetts*,[143] the Supreme Court rejected the argument that there "is a difference, for Confrontation Clause purposes, between testimony recounting historical events, which is 'prone to distortion or manipulation,' and the testimony at issue here, which is the 'resul[t] of neutral, scientific testing."[144] In holding that the Confrontation Clause required an opportunity to cross examine a state expert who vouched for analysis showing a drug to be cocaine, the Court discussed the possibility of flawed forensic tests and

---

139. U.S. CONST. amend. VI.

140. Section IV.E.2, *infra*, explains *"Wade* hearings*."*

141. *See* discussion *supra* Part III.

142. *E.g.*, State v. Kandutsch, 799 N.W.2d 865, 879 (Wis. 2011) *(*citing State v. Armstead, 432 So. 2d 837, 840 (La. 1983)) ("Computer-generated records do not implicate any of [Laurence Tribe's four testimonial] 'infirmities' when the evidence is not the product of human intervention."); *see also id.* (footnote omitted) ("A record created as a result of a computerized or mechanical process cannot lie. It cannot forget or misunderstand. Although data may be lost or garbled as a result of some malfunction, such a malfunction would go to the weight of the evidence, not its admissibility.").

143. 557 U.S. 305 (2009).

144. *Id.* at 317 (quoting Brief for Respondent at 29).

the need for cross examination to ferret out such flaws.[145]

In dissent, Justice Kennedy argued,

> The Confrontation Clause is not designed, and does not serve, to detect errors in scientific tests. That should instead be done by conducting a new test. Or, if a new test is impossible, the defendant may call his own expert to explain to the jury the test's flaws and the dangers of relying on it. And if, in an extraordinary case, the particular analyst's testimony is necessary to the defense, then, of course, the defendant may subpoena the analyst.[146]

The majority holding the opposite view implies that the Confrontation Clause, indeed, empowers cross examination of scientific evidence. But that only gets a defendant so far. When the computer-generated matches themselves are not offered as evidence, challenging the technology faces additional hurdles. First, and most significantly, a motion to exclude the computer-generated matches is not available because they are not being offered into evidence.[147]

As this Article explains repeatedly, law enforcement face-recognition products do not produce a single match, but instead produce an array of possible matches, with probabilities assigned to each image in the array.[148] Because of that limitation on the technology, law enforcement agencies use face-recognition products merely as a first or intermediate step in identification.[149] They present the array output from the computer program to a human witness for more definitive identification.[150] In some cases, the persons identified in the array are physically brought into the presence of the witness for a traditional lineup. In that case, the software is used to select the members of the lineup. In either event, it is the witness identification that is introduced in evidence, not the computer-generated array itself.

---

145. *Id.* at 318–19. *But see* Williams v. Illinois, 567 U.S. 50, 51 (2012) (distinguishing *Melendez-Diaz* and *Bullcoming*, because scientific results in those cases were introduced into evidence).

146. *Melendez-Diaz*, 557 U.S. at 337.

147. Kaitlin Jackson, *Challenging Facial Recognition Software in Criminal Court*, THE CHAMPION, July 2019, at 14, 17–18, https://www.nacdl.org/getattachment/548c697c-fd8e-4b8d-b4c3-2540336fad94/challenging-facial-recognition-software-in-criminal-court_july-2019.pdf [https://perma.cc/JU8E-2DZY].

148. *See supra* text accompanying note 39; Jackson, *supra* note 147, at 17–18 (FBI description of use).

149. *Id.*

150. *Id.* at 17–18.

Therefore, the Sixth Amendment right to confront is involved only indirectly, if at all. The challenger does have an opportunity to confront the witness who made an identification by her own perceptions from whatever the computer program generated. The challenger must sustain the proposition that the Sixth Amendment extends, not only to the witness testimony, but also to the basis for that testimony.

2. Excluding Basis of Testimony Under *Williams v. Illinois*

That argument flies in the face of *Williams v. Illinois*.[151] In that case, a split Supreme Court held that admitting expert testimony based on third-party lab DNA results did not violate the Confrontation Clause. Justice Alito's plurality opinion set the stage for the outcome in its first paragraph:

> In this case, we decide whether *Crawford v. Washington*, 541 U.S. 36, 50 (2004), precludes an expert witness from testifying in a manner that has long been allowed under the law of evidence. Specifically, does *Crawford* bar an expert from expressing an opinion based on facts about a case that have been made known to the expert but about which the expert is not competent to testify? We also decide whether *Crawford* substantially impedes the ability of prosecutors to introduce DNA evidence and thus may effectively relegate the prosecution in some cases to reliance on older, less reliable forms of proof.[152]

The Court summarized what happened:

> In petitioner's bench trial for rape, the prosecution called an expert who testified that a DNA profile produced by an outside laboratory, Cellmark, matched a profile produced by the state police lab using a sample of petitioner's blood. On direct examination, the expert testified that Cellmark was an accredited laboratory and that Cellmark provided the police with a DNA profile. The expert also explained the notations on documents admitted as business records, stating that, according to the records, vaginal swabs taken from the victim were sent to and received back from Cellmark. The expert made no other statement that was offered for the purpose of identifying the sample of biological material used in deriving the profile or for the purpose of establishing how Cellmark handled or tested the sample. Nor did the expert vouch for

151. 567 U.S. 50 (2012).
152. *Id.* at 56.

> the accuracy of the profile that Cellmark produced. Nevertheless, petitioner contends that the expert's testimony violated the Confrontation Clause as interpreted in *Crawford*.[153]

The case did not involve matching by the third-party lab—matching was done by the state police lab personnel who testified. The third-party lab simply produced a DNA profile from the sample sent by the state police, which sample then was compared by the state police with its DNA database.

> On cross examination, Lambatos, the state's expert, confirmed that she did not conduct or observe any of the testing on the vaginal swabs, and that her testimony relied on the DNA profile produced by Cellmark. *Id.* at 59. She stated that she trusted Cellmark to do reliable work because it was an accredited lab, but she admitted she had not seen any of the calibrations or work that Cellmark had done in deducing a male DNA profile from the vaginal swabs. *Id.* at 59–62.[154]

The defense objected, based on lack of foundation for the expert testimony.[155] The Court, noting *Bullcoming v. New Mexico*[156] and *Melendez–Diaz*,[157] held that introducing scientific evidence to prove the truth of the matter asserted therein, without producing the "authors" for cross examination, violated the Confrontation Clause.[158]

The Court then proceeded to explain the purpose of the historical practice of allowing expert witnesses to testify based on hypothetical questions. The hypothetical questions avoided the need to prove the facts underlying the expert's opinion.[159] "Modern rules of evidence continue to permit experts to express opinions based on facts about which they lack personal knowledge, but these rules dispense with the need for hypothetical questions."[160]

The Court narrowed the Confrontation Clause problem. Expert Lambatos's reference to vaginal swabs violated "petitioner's confrontation right because Lambatos lacked personal knowledge that the profile produced by Cellmark was based on the vaginal swabs taken from the victim."[161]

---

153. *Id.* at 56–57.
154. *Id.* at 62.
155. *Id*. at 61.
156. 564 U.S. 647 (2011).
157. 557 U.S. 305 (2009).
158. *Williams*, 567 U.S. at 65–66.
159. *Id.* at 67–69.
160. *Id.* at 69.
161. *Id.* at 72.

The Court acknowledged a significant workaround to the general immunity of lab results forming the basis of expert testimony, referring to FED. R. EVID. 703:

> Under that Rule, 'basis evidence' that is not admissible for its truth may be disclosed even in a jury trial under appropriate circumstances. The purpose for allowing this disclosure is that it may "assis[t] the jury to evaluate the expert's opinion." Advisory Committee's 2000 Notes on Fed. Rule Evid. 703, 28 U.S.C. App., p. 361. The Rule 703 approach, which was controversial when adopted, is based on the idea that the disclosure of basis evidence can help the factfinder understand the expert's thought process and determine what weight to give to the expert's opinion. For example, if the factfinder were to suspect that the expert relied on factual premises with no support in the record, or that the expert drew an unwarranted inference from the premises on which the expert relied, then the probativeness or credibility of the expert's opinion would be seriously undermined.[162]

Independently, the Court articulated a further important exception to the Sixth Amendment, even if the lab evidence had been introduced at trial. This was so because the lab results were not generated "for the purpose of proving the guilt of a particular criminal defendant at trial."[163]

Justice Kagan dissented:[164]

> Under this Court's prior analysis, the substance of the report could come into evidence only if Williams had a chance to cross examine the responsible analyst.
>
> But that is not what happened. Instead, the prosecutor used Sandra Lambatos—a state-employed scientist who had not participated in the testing—as the conduit for this piece of evidence. Lambatos came to the stand after two other state analysts testified about forensic tests they had performed. One recounted how she had developed a DNA profile of Sandy Williams from a blood sample drawn after his arrest. And another told how he had confirmed the presence of (unidentified) semen on the vaginal swabs taken from L.J. All this was by the book: Williams had an opportunity to cross examine both witnesses about the tests they had run. But of course, the State still needed to supply the missing link—it had to show that DNA found in the semen on L.J.'s vaginal swabs matched Williams's DNA. To fill that gap, the

162. *Id.* at 78.

163. *Id.* at 84.

164. *Id.* at 118 (Kagan, J., dissenting).

> prosecutor could have called the analyst from Cellmark to testify about the DNA profile she had produced from the swabs. But instead, the State called Lambatos as an expert witness and had her testify that the semen on those swabs contained Sandy Williams's DNA:
>
> [quoting testimony] . . .
>
> And so it was Lambatos, rather than any Cellmark employee, who informed the trier of fact that the testing of L.J.'s vaginal swabs had produced a male DNA profile implicating Williams.
>
> Have we not already decided this case? Lambatos's testimony is functionally identical to the "surrogate testimony" that New Mexico in *Bullcoming*, which did nothing to cure the problem identified in *Melendez–Diaz* (which, for its part, straightforwardly applied our decision in *Crawford*). Like the surrogate witness in *Bullcoming*, Lambatos "could not convey what [the actual analyst] knew or observed about the events ..., *i.e.*, the particular test and testing process he employed.[165]

She continued with a hypothetical:

> Consider a prosaic example not involving scientific experts. An eyewitness tells a police officer investigating an assault that the perpetrator had an unusual, star-shaped birthmark over his left eye. The officer arrests a person bearing that birthmark (let's call him Starr) for committing the offense. And at trial, the officer takes the stand and recounts just what the eyewitness told him. Presumably the plurality would agree that such testimony violates the Confrontation Clause unless the eyewitness is unavailable and the defendant had a prior opportunity to cross examine him. Now ask whether anything changes if the officer couches his testimony in the following way: "I concluded that Starr was the assailant because a reliable eyewitness told me that the assailant had a star-shaped birthmark and, look, Starr has one just like that." Surely that framing would make no constitutional difference, even though the eyewitness's statement now explains the basis for the officer's conclusion. It remains the case that the prosecution is attempting to introduce a testimonial statement that has no relevance to the proceedings apart from its truth—and that the defendant cannot cross examine the person who made it. Allowing the admission of this evidence

165. *Id.* at 123–24.

> would end-run the Confrontation Clause, and make a parody of its strictures.
>
> And that example, when dressed in scientific clothing, is no different from this case. The Cellmark report identified the rapist as having a particular DNA profile (think of it as the quintessential birthmark). The Confrontation Clause prevented the State from introducing that report into evidence except by calling to the stand the person who prepared it. See *Melendez–Diaz*, 557 U.S., at 310–311, 129 S. Ct. 2527; *Bullcoming*, 564 U.S., at ——, 131 S. Ct., at 2709–2710. So the State tried another route—introducing the substance of the report as part and parcel of an expert witness's conclusion. In effect, Lambatos testified (like the police officer above): "I concluded that Williams was the rapist because Cellmark, an accredited and trustworthy laboratory, says that the rapist has a particular DNA profile and, look, Williams has an identical one." And here too, that form of testimony should change nothing. The use of the Cellmark statement remained bound up with its truth, and the statement came into evidence without any opportunity for Williams to cross examine the person who made it. So if the plurality were right, the State would have a ready method to bypass the Constitution (as much as in my hypothetical case); a wink and a nod, and the Confrontation Clause would not pose a bar to forensic evidence.[166]

Justice Kagan's dissent noted that the fragmented character of the court's decision eliminates clear guidance from the three-person Alito plurality, and the concurring opinions of Justice Breyer and Justice Thomas each offer a different rationale for why the defendant was not entitled to cross examine the authors of the lab report.[167] That lack of clarity has enabled state courts to craft their own paths. *State v. Watson*[168] is a good example. The New Hampshire Supreme Court embraced Justice Kagan's observation, and limited *Williams* to its facts.[169] It held that the defendant could cross examine the principal author of a lab report.[170]

On the other hand, the New Hampshire Supreme Court implicitly embraced Justice Breyer's argument about the practical limitation on allowing cross examination of everyone who participated in generating lab reports.[171] As Justice Breyer observed, most sophisticated forensic

166. *Id.* at 127–28.
167. *Id.* at 120 ("five votes . . . but not a single good explanation").
168. 185 A.3d 845 (N.H. 2018).
169. *Id*. at 855–56.
170. *Id*. at 857.
171. *See id*. at 859.

investigations involving DNA evidence involve participation by multiple technicians and experts. Concluding that lab results are not admissible without allowing cross examination of each person would significantly impede the utility of technological evidence that ordinarily is valuable for fact-finding.[172]

The *Watson* court thus drew the line at mandating the availability of everyone participating in laboratory analysis once the principal investigator had testified and been made available for cross examination.

> [T]he report in this case, from a private laboratory, was admitted through the testimony of Isenschmid, the forensic toxicologist who issued and signed it and who was available for cross examination.
>
> . . . .
>
> In this case, Isenschmid reviewed 'all the documentation' in the case, including the chain of custody, and ensured that all of the information had been correctly entered into the NMS computer system. Isenschmid personally reviewed the 'actual instrument data' and made sure that the data were accurately entered into the NMS computer. Further, he 'actually reviewed all of the testing results.' He also issued and signed the toxicology report that described the testing results and testified that the report accurately reflected his findings and conclusions. His 'participation in preparing the report and developing the substantive conclusions contained therein was real and direct.'[173]

The Watson court noted, "[a]lthough contrary authority exists, we note that our decision today comports with those of at least seven federal courts and 21 state courts, which, in opinions issued since 2012, have found no Confrontation Clause violation under similar circumstances."[174]

A further limitation on extending the holding in *Williams* broadly is the limited nature of the laboratory investigation in that case, combined with indicia of reliability other than cross examination of the lab investigators.[175] Constructing a DNA profile from the samples submitted to the lab was a relatively narrow and mostly straightforward task routinely done in the industry. The chain of custody of the sample submitted to the lab was established by in-court testimony, which adequately tested the possibility that the lab analyzed a sample belonging

---

172. *See Williams*, 567 U.S. at 89 (Breyer, J., concurring).

173. *Watson*, 185 A.3d at 858 (distinguishing *Bullcoming* and *Melendes-Diaz*).

174. *Id.* at 859 (footnotes omitted).

175. *See Williams*, 567 U.S. at 74–75; *but see* Crawford v. United States, 541 U.S. 36, 64–69 (2004) (rejecting reliability exception to Confrontation Clause).

to someone else.[176] The in-court testimony of the state police expert established that contamination of the sample used in the analysis would have been readily apparent in the results. Given this, cross examination would not have had much value in probing reliability. The remaining non-transparency of the laboratory process was covered by the business records exception to the hearsay rule: reliable because routinely relied on.[177]

Computerized face-recognition analysis is quite different from the laboratory analysis that escaped cross examination in *Williams*. Face-matching methodologies are not yet in routine use: they are both quite new and are currently being proven. This makes the business records exception a poor fit.

Moreover, multiple decisions must be made in developing and using computerized face-matching software. Each decision requires specialized expertise and judgments about costs and benefits. Designers make decisions about which algorithms to use based on an understanding of the marginal utility of the algorithms and their error rates. Designing and maintaining the database similarly requires expertise and judgments about what images should be included in the database to make it representative of the relevant population. The users of the database also must determine the threshold quality standards for an image before it can be included in the database. These matters go far beyond the relatively routine decisions made in extracting the DNA profile from one sample. Each of these judgments affects the overall reliability of a resulting match, and the argument is strong that an opponent of the evidence should be able to probe each of the elements of the matching process through cross examination.

On the other hand, the plurality's conclusion in *Williams* that the laboratory test results were not testimonial,[178] agreed to by Justice Thomas[179] and Justice Breyer,[180] would apply as well to *one unknown to many knowns* face-matching, not intended initially to prove that anyone committed a crime. Normally, the purpose of a one unknown to many knowns face-matching is to identify someone who may have committed a crime, not to prove that the person committed it.

> The Cellmark report is very different [from the reports in *Melendez–Diaz* and *Bullcoming*]. It plainly was not prepared for the primary purpose of accusing a targeted

176. *See Williams*, 567 U.S. at 74 (finding little room for argument that sample came from any source other than the victim's vaginal swabs).

177. *See id*. at 99 (Breyer, J., concurring) (referring to business records exception to hearsay rule).

178. *See id*. at 84 (plurality opinion).

179. *Id*. at 103–04 (Thomas, J., concurring).

180. *Id*. at 93 (Breyer, J., concurring).

> individual. In identifying the primary purpose of an out of court statement, we apply an objective test. We look for the primary purpose that a reasonable person would have ascribed to the statement, taking into account all of the surrounding circumstances.
>
> Here, the primary purpose of the Cellmark report, viewed objectively, was not to accuse petitioner or to create evidence for use at trial. When the ISP lab sent the sample to Cellmark, its primary purpose was to catch a dangerous rapist who was still at large, not to obtain evidence for use against petitioner, who was neither in custody nor under suspicion at that time. Similarly, no one at Cellmark could have possibly known that the profile that it produced would turn out to inculpate petitioner—or for that matter, anyone else whose DNA profile was in a law enforcement database. Under these circumstances, there was no 'prospect of fabrication' and no incentive to produce anything other than a scientifically sound and reliable profile.
>
> The situation in which the Cellmark technicians found themselves was by no means unique. When lab technicians are asked to work on the production of a DNA profile, they often have no idea what the consequences of their work will be. In some cases, a DNA profile may provide powerful incriminating evidence against a person who is identified either before or after the profile is completed. But in others, the primary effect of the profile is to exonerate a suspect who has been charged or is under investigation. The technicians who prepare a DNA profile generally have no way of knowing whether it will turn out to be incriminating or exonerating—or both.[181]

This lack of focus on a particular individual was crucial to the Supreme Court's analysis of testimonial purpose and is true, as well, of the one unknown to many knowns face-matching analysis.

The conflicted character of the reasoning in *Williams*, however, makes its application to face-recognition uncertain, even in federal court. Application of the case and its reasoning is even less certain in state courts, where protections of the right to cross examine may differ from those of the Sixth Amendment. State courts also may feel freer to test the limits of the *Williams* case, as they did in *Watson*.

3. Computerized Face-Matching as Basis for Testimony

The plurality in *Williams* observed: "This conclusion will not prejudice any defendant who really wishes to probe the reliability of the

181. *Id*. at 84–85 (internal citations omitted).

DNA testing done in a particular case because those who participated in the testing may always be subpoenaed by the defense and questioned at trial."[182] So, finding a computerized face-match to be outside the Confrontation Clause does not resolve the question whether the defense has independent access to it for cross examination.

Federal Rule of Evidence 705 requires experts to disclose, on cross examination, facts or data that underlie the expert's opinion.[183] Many state evidence rules have similar requirements.[184] Rule 703 makes the basis of an expert's opinion admissible, even if it is not independently admissible, to aid the fact finder in evaluating the expert's testimony.[185] The requirement that the court balance probative value against prejudicial effect is relaxed when the basis is introduced by a party opposing the expert.[186] The commentary to the original, 1975 version of the rule encourages its use to decide admissibility based on "the validity of the techniques employed rather than to relatively fruitless inquiries whether hearsay is involved."[187] The quoted language is explicitly related to public opinion poll evidence, but its logic extends to any kind of basis evidence, including computerized face-recognition.

"Opinions are valueless as evidence without exploration of the underlying facts and rationale showing the path from the facts to the opinion," as one court said.[188]

Bauer v. Bayer A.G.,[189] is a good example of the kind of judicial scrutiny of the basis for an expert's opinion that is permissible. The case involved a products liability claim against an insecticide manufacturer by beekeepers who claimed the product killed their bees. The court excluded the defendant's expert testimony because the testing protocol relied on by the expert was not shown to have "adequate scientific support,"[190] although expert testimony is generally allowed when it is based on the type of data on which experts reasonably rely:[191]

> The reliability of the initial ADPEN analysis is undermined by the unexplainable level of imidacloprid found in the control sample (153.6 ppb), especially considering that the control sample was assumed clean and

182. *Id*. at 58–59.
183. FED. R. EVID. 705.
184. FED. R. EVID. 705 advisory committee note to 1972 proposed rules.
185. FED. R. EVID. 703.
186. FED. R. EVID. 703 advisory committee note to 2000 amendments.
187. FED. R. EVID. 703 advisory committee note to 1972 proposed rules.
188. United States v. R. J. Reynolds Tobacco Co., 416 F. Supp. 316, 325 (D.N.J. 1976).
189. 564 F. Supp. 2d 365, 374–75 (M.D. Pa. 2008).
190. *Id.* at 368.
191. *Id.* at 376.

> devoid of any imidacloprid. Dr. William Leimkuehler, in a detailed critique, remarked that a finding of such a concentration in the control sample suggests a molecule other than imidacloprid was being measured. Dr. Scott–Dupree affirmed, stating that some type of problem was present in the test method. Dr. Mayer, likewise, was at a loss to explain such a high level of imidacloprid in the control: "It's unexplained. I can't explain it. I mean it happened."[192]

The record contained extensive testimony by witnesses on both sides regarding the reliability of the underlying tests.

4. Fourth Amendment

The Fourth Amendment prohibits searches and seizures not supported by probable cause, or not authorized by a warrant supported by probable cause. The scope of Fourth Amendment protection is determined by an individual's "reasonable expectation of privacy"—or a property interest protected against trespass.[193] One has a reasonable expectation of privacy in his DNA while it is still contained within his body, but not in the fingerprints that he leaves everywhere. People do not have a reasonable expectation of privacy in their appearance, including their faces, which are usually exposed for the world to see.[194]

Thus, Fourth Amendment analysis of the big three types of biometric evidence differs. Superficially, an argument that collecting facial images for use either as probe images or for inclusion in a training or enrolled database is frivolous. Such collection may, however, violate state statutory law, such as the Illinois statute considered in Section IV.C. It also may be subject to Fourth Amendment limitations when it divests subjects of anonymity by revealing their patterns of activity.

---

192. *Id.* at 377.

193. *See* United States v. Jones, 565 U.S. 400, 404–09 (2012) (holding that placement of GPS tracking device was a search under the Fourth Amendment because it was trespassory; explaining duality of reasonable-expectation-of-privacy and property bases for protection); Florida v. Jardines, 569 U.S. 1, 8–9 (2013) (holding that dog sniff on front porch was a Fourth Amendment search because it was a trespass).

194. Justice Scalia emphasized the point in his dissent in *Maryland v. King*:§

> Is not taking DNA samples the same, asks the Court, as taking a person's photograph? No—because that is not a Fourth Amendment search at all. It does not involve a physical intrusion onto the person, and we have never held that merely taking a person's photograph invades any recognized "expectation of privacy." Thus, it is unsurprising that the cases the Court cites as authorizing photo-taking do not even mention the Fourth Amendment.

569 U.S. 435, 476–77 (2013) (Scalia, J., dissenting) (citations omitted).

Fourth Amendment analysis is considerably different for DNA and face-matching. Obtaining a subject's DNA is a Fourth Amendment search, and thus unconstitutional unless performed pursuant to a warrant or is otherwise reasonable. If the officer obtains DNA from a blood sample, a urine sample, or a saliva sample, then the Fourth Amendment applies. On the other hand, if the DNA has been left behind, on a drinking cup or eating utensils, obtaining a DNA sample from those sources is not a search.

Capturing someone's image is not a search because one has no reasonable expectation of privacy in one's unconcealed face. So, if the police officer is near a suspect and takes his picture with a cell phone, that act does not encounter Fourth Amendment limitations.[195]

Obtaining fingerprints, like obtaining photographs of faces, may not involve searches, although detention of a subject long enough to get fingerprints or a photo may involve a Fourth Amendment seizure.

a. Acquiring DNA

Both DNA-matching and face-matching involve biometric evidence and computerized searching. But obtaining DNA evidence involves more intrusion than taking someone's photograph.

In *Maryland v. King*,[196] the Supreme Court held, 5-4, that a post-arrest DNA swab was reasonable under the Fourth Amendment. The defendant was arrested for another offense and, as part of the routine booking procedure, a sample of his DNA was obtained by swabbing the inside of his cheeks. The DNA matched a sample in a state DNA database that was taken from a rape victim six years prior to the arrest. The Maryland Court of Appeals reversed his conviction for rape, holding that the DNA swab was an unlawful search under the Fourth Amendment.[197]

The Supreme Court agreed that taking the DNA swab constituted a Fourth Amendment search.[198] The search was reasonable, however, because it was: (1) incident to an arrest; (2) a routine part of the booking process; and (3) strictly limited by the applicable state statute.[199] Both the majority and dissenting opinions in *Maryland v. King* noted the

---

195. *But see* Fretty, *supra* note 46 (arguing that Fourth Amendment protects commercially held databases of faces, such as Facebook's from governmental search); Nguyen, *supra* note 58, at *34–53 (arguing that reconceptualized Fourth Amendment and First Amendment right of anonymity can limit police use of face-recognition technology).

196. 569 U.S. 435 (2013).

197. *Id.* at 439–41 (giving factual and procedural history).

198. *Id.* at 446 (noting that caselaw treats drawing blood, scraping fingernails, and breathalyzer tests as Fourth Amendment searches; holding that a buccal DNA swab is also a Fourth Amendment search).

199. *Id.* at 449–50; *see also id.* at 465 (detailing statutory restrictions).

ubiquitous use of DNA matching as a criminal investigation tool.[200] The modesty of the intrusion was an important element in the Court's reasonableness analysis.[201] Balanced against the modest intrusion was the government's interest in confirming the identity of an arrestee and obtaining an accurate criminal history.[202]

Justice Scalia, joined by Justices Ginsberg, Sotomayor, and Kagan, dissented.[203] His principal concern was the majority's refusal to require an individualized suspicion focused on the target of the search.[204] He rejected the justification that the DNA was used only to identify the suspect, arguing that it was instead used to search for evidence that the arrestee had committed crimes other than those for which he was arrested.[205] He noted that the DNA search that occurred involved matching the defendant's sample against the "unsolved crimes" database, not a broader database of all convicts and arrestees, further belying the identification purpose.[206] Some states, such as Vermont, disagree with the *Maryland v. King* conclusion and hold that DNA searches violate state constitutions.[207]

The DNA cases make it clear that taking a mugshot incident to an arrest and using it as a face-recognition probe image is reasonable under the Fourth Amendment: taking a picture is not a search at all; the intrusion is minimal; and the need for identification the same. The evolving DNA caselaw also contains the seeds of possible restrictions on searching enrolled databases, and the statutory limitations on collection and use of DNA samples in the *Maryland v. King* and post-*Maryland* cases are plausible models for similar limitations on face-recognition.

b. Acquiring Fingerprints

The Fourth Amendment plays a weaker role with respect to fingerprint evidence than it does with respect to DNA evidence. That is because obtaining DNA from an unwilling subject is more intrusive than obtaining fingerprints—an arguable proposition—and because the expectation of privacy in one's DNA is greater than in one's fingerprints. One leaves replicas of one's fingerprints on everything he or she touches.

---

200. *Id.* at 445–46 (describing CODIS, a national U.S. standard for comparing DNA, resulting in high reliability of matches, on the order of 1 in 100 trillion).

201. *Id.* at 462.

202. *Id.* at 450–56.

203. *Id.* at 466 (Scalia, J., dissenting).

204. *Id.* at 469–70; *see also id.* at 448 (majority opinion) (internal quotation marks and citation omitted) ("[T]he touchstone of the Fourth Amendment is reasonableness, not individualized suspicion.").

205. *Id.* at 469–70 (Scalia, J., dissenting).

206. *Id.* at 473–74.

207. *See* State v. Medina, 102 A.3d 661, 683 (Vt. 2014).

That is less true with DNA, although one does leave DNA traces on cigarette butts, drinking cups, and eating utensils.[208]

The law of fingerprints is relevant to developing the law of computerized face-matching because: (a) fingerprints, like facial images, are biometric evidence; (b) obtaining fingerprints, if it constitutes a search at all, requires no more than *Terry* reasonable suspicion; (c) fingerprint matches generally are admitted into evidence; (d) fingerprint matching is, at least partially, automated; and (e) rules for authenticating and cross examining fingerprint evidence are highly developed.

Fingerprinting of arrestees generally is accepted as legal,[209] although Justice Scalia noted, in his dissent, in *Maryland v. King*, that "our cases provide no ready answer" to the question whether taking fingerprints constitutes a search. "The 'great expansion in fingerprinting came before the modern era of Fourth Amendment jurisprudence,' and so we were never asked to decide the legitimacy of the practice."[210]

In *Hayes v. Florida*,[211] the Supreme Court applied *Davis v. Mississippi*[212] to hold that transporting a suspect to the police station and detaining him there to obtain fingerprints without probable cause or a warrant violated the Fourth Amendment. The Fourth Amendment violation occurred because of the seizure of the suspect, not because fingerprinting is a search. The Court hedged, however: "None of the foregoing implies that a brief detention in the field for the purpose of fingerprinting, where there is only reasonable suspicion not amounting to probable cause, is necessarily impermissible under the Fourth Amendment."[213]

---

208. In Commonwealth v. Arzola, the Massachusetts Supreme Judicial Court held that obtaining a DNA sample from a bloodstain on a shirt that had been lawfully seized did not constitute a search. 26 N.E.3d 185, 191–92 (Mass. 2015) (comparing it to use of latent fingerprints; suggesting that more extensive analysis of DNA might be a search because it would invade a reasonable expectation of privacy); *see also* State v. Williford, 767 S.E.2d 139, 144 (N.C. Ct. App. 2015) (holding that search of DNA extracted from cigarette butt was not a search, distinguishing *King* and citing cases from other states).

209. *King*, 569 U.S. at 458 (restating longstanding conclusion that fingerprinting is reasonable because it is part of the usual administrative steps incident to arrest).

210. *Id.* at 479 (Scalia, J., dissenting) (noting that the early fingerprinting cases were decided before the Fourth Amendment was made applicable to the states).

211. 470 U.S. 811 (1985).

212. 394 U.S. 721 (1969).

213. *Hayes*, 470 U.S. at 816.

Under the reasoning of *Terry v. Ohio*,[214]

> There is thus support in our cases for the view that the Fourth Amendment would permit seizures for the purpose of fingerprinting, if there is reasonable suspicion that the suspect has committed a criminal act, if there is a reasonable basis for believing that fingerprinting will establish or negate the suspect's connection with that crime, and if the procedure is carried out with dispatch. Cf. *United States v. Place*, *supra.* Of course, neither reasonable suspicion nor probable cause would suffice to permit the officers to make a warrantless entry into a person's house for the purpose of obtaining fingerprint identification.[215]

Justice Brennan concurred in the judgment, expressing doubt about on-site fingerprint detentions:

> If the police wanted to detain an individual for on-site fingerprinting, the intrusion would have to be measured by the standards of *Terry v. Ohio*, 392 U.S. 1 (1968), and our other Fourth Amendment cases. Yet the record here contains no information useful in applying *Terry* to this hypothetical police practice. It would seem that on-site fingerprinting (apparently undertaken in full view of any passerby) would involve a singular intrusion on the suspect's privacy, an intrusion that would not be justifiable (as was the pat down in *Terry*) as necessary for the officer's protection. How much time would elapse before the individual would be free to go? Could the police hold the individual until the fingerprints could be compared with others? The parties did not brief or argue these questions, the record contains nothing that is useful in their resolution, and (naturally enough) the courts below did not address them.[216]

c. Acquiring Photographs

This caselaw persuasively supports the proposition that law enforcement officers are privileged to stop a person long enough to take a picture of his face—a process that would involve a much briefer

---

214. 392 U.S. 1, 30–31 (1968) (allowing stop and frisk on reasonable suspicion, less than probable cause).

215. *Hayes*, 470 U.S. at 817.

216. *Id.* at 818–19 (Brennan, J., concurring in judgment); *see also* Beaver, *supra* note 26 ("Our [Indiana State] Troopers . . . [who] had access to portable fingerprint scanners . . . could scan databases within minutes. I never used one but my impression was they [took] less than 10 minutes or so to get a return, if any, though you'd have to have one on scene, and extending a stop to get one there may exceed what is allowed by the 4th Amendment.").

detention than stopping him long enough to fingerprint him. Mugshots are a common source of a probe image for face-matching systems. If capturing such an image qualified as a Fourth Amendment search, the Constitution would limit face-matching just like it limits DNA matching. However, taking a mugshot is not a Fourth Amendment search.

The Supreme Court, in *Maryland v. King*, approved the use of photography as a tool of criminal investigation.[217] "Police had been using photography to capture the faces of criminals almost since its invention."[218] Justice Scalia noted in his dissent that taking a person's photograph is not a Fourth Amendment search at all, because it does not involve a physical intrusion into a person and because it does not invade any recognized expectation of privacy.[219]

d. Patterns of Movement

A more sophisticated argument under the Fourth Amendment considers the expectation of privacy in facts that, while discretely public, *collectively* reveal aspects of one's life that traditionally were not open to public knowledge. Cell phone tracking information falls into this category and thus is clothed with a reasonable expectation of privacy, according to *Carpenter v. United States*.[220]

> A person does not surrender all Fourth Amendment protection by venturing into the public sphere. To the contrary, what one seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.[221]
>
> Allowing government access to cell-site records contravenes that expectation. Although such records are generated for commercial purposes, that distinction does not negate Carpenter's anticipation of privacy in his physical location. Mapping a cell phone's location over the course of 127 days provides an all-encompassing record of the holder's whereabouts. As with GPS information, the time-stamped data provides an intimate window into a person's life, revealing not only his particular movements, but through them his familial, political, professional, religious,

217. Maryland v. King, 569 U.S. 435, 451 (2013) (noting generally accepted processes of comparing booking photograph with sketch artist images and showing photos to witnesses, and matching fingerprints).

218. *Id.* at 456–57.

219. *Id.* at 477 (Scalia, J., dissenting).

220. 138 S. Ct. 2206, 2217–19 (2018) (holding that venturing into public sphere does not negate expectation of privacy in movements revealed by historical cell site data); *see also* United States v. Elmore, 917 F.3d 1068, 1074 (9th Cir. 2019) (applying *Carpenter* and finding no probable cause).

221. *Carpenter*, 138 S. Ct. at 2217.

> and sexual associations. These location records hold for many Americans the privacies of life. And like GPS monitoring, cell phone tracking is remarkably easy, cheap, and efficient compared to traditional investigative tools. With just the click of a button, the Government can access each carrier's deep repository of historical location information at practically no expense.
>
> In fact, historical cell-site records present even greater privacy concerns than the GPS monitoring of a vehicle we considered in *Jones*. Unlike the bugged container in *Knotts* or the car in *Jones*, a cell phone [is] almost a "feature of human anatomy."[222]

A face *is* a feature of human anatomy. It follows its owner everywhere. Logically, one can extend the reasoning in *Carpenter* to faces captured from people who are in a crowd or a queue and relatively anonymous there. To take their pictures and use the pictures to identify them divests these people of the anonymity of which they had a reasonable expectation. But one must be meticulous in drawing the analogy between computerized face-recognition and access to cellphone location records. Is it the mere taking of a photograph of a stranger's face that constitutes the search? Probably not. That does not compromise anonymity or privacy. It is the subsequent use of the captured image to search a database that identifies the individual. Even then, no pattern of movement or conduct is revealed unless an individual is repeatedly identified by his face and accordingly tracked for a significant period of time.

e. Incident to Arrests

When fingerprints, DNA, or photographs are obtained after an arrest, probable cause for the arrest has already been determined.[223] Thus, whether a separate warrant is necessary for post-arrest searches presents a slightly different question from pre-arrest searches. A regular part of the booking process whenever someone is arrested involves taking a mugshot. Even if that is a search, it is incident to an arrest. If the arrest is lawful, the search is lawful.

E. *Challenging Reliability of Traditional Witness Identification*

The law of conventional pre-trial identification procedures is relevant to computerized face-matching because computerized face-matching, with the current state of the technology, is used pre-trial rather than

---

222. *Id.* at 2217–18 (internal quotations and citations omitted).

223. *King*, 569 U.S. at 448 (noting that post-arrest obtaining of DNA involves situation where probable cause already is established).

providing a face-match that is directly introduced into evidence. Accordingly, the legal doctrines giving defendants an opportunity to go behind the in-court witness identification to probe the effect of pre-trial identification procedures including lineups, show ups, and photo arrays, is material to a defendant's argument that he should be able to go behind in-court witness identification to probe computerized face-matches that were shown to the witness before trial.

Beyond that, the concept of suggestiveness—the heart of challenges to witness identification based on pre-trial procedures—can be used as one of several techniques for scrutinizing computerized face-matching.

This Section analyzes the case law involving suggestiveness and applies it to computerized face-matching. It considers the threshold requirements for, and the content of, "*Wade* hearings," which afford defendants an adversarial opportunity to challenge pre-trial identification techniques, which logically include computerized face-matching. Then, the ection briefly considers the law involved when a computerized face-match is not shown to a witness but used instead to generate a wanted poster.

Challenges to witness identification based on pre-trial techniques such as lineups, show ups, and photo arrays obviously are relevant to formulating challenges to pre-trial computerized face-matches. Two other kinds of forensic evidence also inform consideration of computerized face-matches as evidence: fingerprint matches and DNA matches. With all three, as with computerized face-matches, the fundamental question is whether they are sufficiently probative to be shown to the factfinder.[224] They differ, however, in indicia of their probativeness. A DNA match results from out of court use of sophisticated chemical analysis. Fingerprint matches depend on out of court human analysis of physical artifacts of fingerprint patterns, increasingly aided by computer routines. The points that indicate a match can be illustrated easily in court by diagrams. DNA matches and fingerprint matches are admitted into evidence only when they are presented by an expert witness who introduces and explains them and is subject to cross examination about the out of court processes. In contrast, the role of lineups, show ups, and photo arrays are frequently obscured because the witness who participated in them comes into court and makes a new, live identification of the defendant.

Computerized face-matching most closely resembles the lineup, show up, and photo array category because both ask whether a face produced

224. Subordinate inquiries over reliability, authentication, hearsay exclusion, and the overarching question of relevancy all have to do with probativeness. Relevancy weighs probativeness against prejudicial effect. Authentication enforces probativeness by insisting that evidence be what it is claimed to be. Hearsay exclusions reject evidence whose probativeness cannot be tested in court by cross examination. Reliability is just another word for probativeness.

out of court is likely to be the face of the defendant, but like traditional face-identification, and unlike fingerprints and DNA, the prosecution may introduce face identification evidence by live witness testimony without reference to the out of court process.

In *United States v. Wade*, however, the Supreme Court pointed out an important difference between witness identification and fingerprints, blood, clothing, and hair samples.[225] For all of these except witness identification,

> [k]nowledge of the techniques of science and technology is sufficiently available, and the variables in techniques few enough, that the accused has the opportunity for a meaningful confrontation of the Government's case at trial through the ordinary processes of cross examination of the Government's expert witnesses and the presentation of the evidence of his own experts.[226]

The Court was concerned with whether the constitutional right to counsel extended to the pre-trial investigatory stages of a prosecution. It held that it does extend to face-recognition, but not to fingerprint, blood, clothing, and hair matching evidence. (DNA matching was not in general use when the Supreme Court decided *Wade*). The Court's logic was that scientific evidence is *more* reliable than witness identification.

Computerized face-matching differs from the traditional categories of scientific evidence in two important ways. First, its techniques are less generally known and the variables in techniques large enough that the consensus that backs up good practice in fingerprint and DNA analysis is lacking regarding computerized face-matching. Second, computerized face-recognition differs from fingerprint and DNA identification in that computerized face-recognition deals with artifacts that can be evaluated by an ordinary human being. Fingerprint identification requires training and skill in singling out the features of fingerprints that distinguish them from others. This is not something within the ken of ordinary people, and it is not something that can be done without the aid of a microscope and pre-recorded fingerprints. DNA identification requires knowledge of how genetic material is arranged and the particular sequences that collectively make a sample from an individual unique. None of this is within the knowledge possessed by ordinary citizens, and it relies on data that can be perceived only with the aid of sophisticated chemical analysis.

Not so with face-recognition; everyone looks at facial features and identifies faces dozens or hundreds of times a day. While most people would not be very articulate about how they know that a face belongs to

225. United States v. Wade, 388 U.S. 218, 227–28 (1967).

226. *Id.* at 227–28.

a particular person, they instinctively process facial artifacts with great accuracy.

These important differences between face-recognition and the two other most used forms of forensic identification have large implications for reliability of evidence introduced in court. First, they make it more difficult to cross examine the proponent of computerized face-matching. Second, computerized face-matching process may not even be in evidence, a lay witness has made an allegedly independent identification. Undermining the reliability is the possibility that computerized face-matching has been used to construct matches that are then presented to a human witness to ratify. Only the testimony of the human witness is introduced into evidence and subject to cross examination. How the material from which the witness worked was constructed is not offered in court and likely is immune from cross examination. Depending on the criminal discovery rules in a particular jurisdiction, the use of computerized face-matching may not even be revealed or disclosed to the defendant. On the other hand, the defense's right to cross examine a witness about lineups, show ups, or photo arrays implies that a defendant should similarly be able to cross examine with respect to computer-generated arrays.

Still, the combination of computerized face-matching and witness testimony enhances reliability. Human intervention between the computerized matching and the identification imposes a reality check on the computer process. A human witness may look at the image that the computerized algorithm thinks represents a match and say, "No. That's not the guy. It does not look anything like him." Such lay testimony is unavailable as a reality check against fingerprint or DNA evidence. The intervention of the computer algorithms between the event and the in-court witness identification removes the possibility of human bias that so often taints conventional, lineups, show ups, and photo arrays.

Because eyewitness identification is notoriously unreliable,[227] the law has developed a variety of techniques to expose instances in which its accuracy is questionable. Those tools for evaluating reliability include all the methods accepted for challenging witness identification based on lineups, show ups, and photo arrays. When computerized face-matching algorithms are used as a foundation for witness identification, their use

227. "The identification of strangers is proverbially untrustworthy." *Id.* at 228 (quoting Felix Frankfurter, *The Case of Sacco and Venzetti*, THE ATLANTIC, Mar. 1927, https://www.theatlantic.com/magazine/archive/1927/03/the-case-of-sacco-and-vanzetti/306625/ [https://perma.cc/S4Q7-UEK4]) (holding that defendant is entitled to be represented by counsel at lineup); *accord* State v. Guilbert, 49 A.3d 705, 720–30 (Conn. 2012) (discussing scientific evidence showing unreliability of eyewitness identification and holding that expert testimony to that effect is admissible).

should be subject to scrutiny, just like the construction of the lineup, show up, or photo array.

Computerized face-recognition presents the same legal issues as other identification techniques long used in criminal cases. The law for face-recognition accordingly tracks the law developed for the other technologies. *Suggestiveness* is the key concern, accompanied by other facts that cast doubt on human witness identification.

1. Suggestiveness

All identification involves comparisons of crime scene data with data obtained later from the defendant. Crime scene data typically is imperfect: only partial fingerprints; only a slight amount of DNA; only a brief glimpse at the robber, whose hoodie partially concealed his face; surveillance imagery was out of focus, grainy, and the robber had his head partially turned. In contrast the later-acquired data—fingerprints, DNA specimens, or images—are as nearly perfect as the investigators want to make them.

Traditional identification based on appearance usually involves a witness to the crime who testifies, at the trial of the defendant, that the defendant is the person who robbed her. Like any identification, this involves a comparison of what was seen or photographed at the time of the crime with the later appearance of the defendant. The identification may be flawed for one of three reasons. First, the initial perception of the perpetrator may have been limited because the perpetrator was wearing a disguise, because the victim could not see him clearly, or because the victim's emotional state prevented the perpetrator's appearance from registering fully.[228] Second, the image that the defendant presents in court may be different from the image presented at the time of the crime because of changed facial hair, substantial weight loss or weight gain, or other physical changes. Third, the witness's recollection of the image from the time of the crime may be imperfect because memory fades with time and, more importantly, because later experiences compete with the original perception. It is this third source of the error that attracts the most litigation over eyewitnesses' identifications. A defendant claims that the witness has seen many other faces since the crime and that this naturally blurs the clarity of her recollection. The defendant will cross examine to adduce anything that might give a later facial image particular significance to the witness, thereby causing the witness to conflate the earlier-in-time image with the later one. This is the concept of suggestiveness. Suggestiveness would occur, for example, if the witness

228. *See Guilbert*, 49 A.3d at 715–16 (discussing expert testimony on effect of stress in reducing reliability of witness identification and that that accuracy of identification may be adversely affected by such factors as the length of time during which the eyewitness was able to observe the person, lighting, distance, and whether the eyewitness was paying attention).

got only a momentary view of the robber before she was knocked out. During the brief time she saw the robber, she was so terrified she thought she might faint. It was dark. The robber was wearing a hoodie pulled tight over his forehead, cheeks, and chin. Later, investigators bring a suspect into an interview room and put the witness on the other side of a one-way mirror through which she can see the suspect. The interview room is well lit, and the witness is allowed plenty of time to examine the suspect. An investigator tells the witness: "We're almost certain this is the guy. Do you recognize him?" The image of the suspect in the show up is going to be burned into the witness's mind much more clearly than that of the actual perpetrator. The witness goes to the court. The suspect is at the defense table, and the witness identifies him, based more on the show up than on what she saw during the crime.

The hypothetical presents an extreme example of suggestiveness, of course, but the possibilities for suggestiveness are endless. The police rush out from the crime scene and bring somebody back that they apprehended nearby and present him to the witness; the police organize a lineup or a photographic array in which one of the faces is different from all the others; the police show the witness a computerized face-match and tell the witness it is the product of a computer algorithm and artificial intelligence. Once a witness has picked out a subject in a lineup, show up, or photo array, she is not likely to go back on her word at trial.[229] So suggestiveness of the pre-trial technique undermines the reliability of the in-court testimony.

In *Bernal v. People*,[230] the Colorado supreme court explained the analytical framework for evaluating the admissibility of identifications from photo arrays:

> This standard [for suggestiveness, under *Simmons v. United States*, 390 U.S. 377 (1968)] has developed into a two-part analysis. First, a court must determine whether the photo array was impermissibly suggestive, which the defendant has the burden of proving. If this burden is not met, no further inquiry is necessary. Second, if the defendant's burden is met, the burden shifts to the People to show that despite the improper suggestiveness, the identification was nevertheless reliable under the 'totality of the circumstances.' It is important to note that these two steps must be completed separately; it is only necessary to reach the second step if the court first determines that the array was impermissibly suggestive.
>
> In evaluating whether a pre-trial photo identification procedure is impermissibly suggestive, a number of factors

229. *Wade*, 388 U.S. at 229.

230. Bernal v. People, 44 P.3d 184, 191 (Colo. 2002).

> may be relevant. These include the size of the array, the manner of its presentation by the officers, and the details of the photographs themselves. Although courts have held that a photo array with as few as six pictures is not per se a due process violation, courts have recognized that the size of a photo array, specifically the number of pictures in it, is a factor affecting the weight a court gives to the irregularities in the array. The more pictures used in an array, the less likely it is that a minor difference, such as background color or texture, will have a prejudicial effect on selection.
>
> In contrast, when relatively few photographs are used in an array, minor differences such as background color, make a picture stand out and can repeatedly draw a witness's eyes to that picture.

Id. In *Sanchez*, the court noted:

> Common sense dictates that slight irregularities are more likely to 'jump out' at a witness when reviewing a single sheet of paper with only six photographs on it than at a witness reviewing a large mug book containing hundreds of photographs. Upon continued inspection, the witness may begin to believe that the 'oddball' picture was taken under different circumstances than the others. This fact can suggest a number of things to the witness, the most dangerous of which is that the similar pictures were taken together to form a pool or control group, and that the one picture that stands out is the suspect.
>
> Thus, the fewer photographs used by the officers in a photo array, the closer the array must be scrutinized for suggestive irregularities.
>
> When the number of photographs shown has not been so small as to make the presentation itself unfairly suggestive, and there is nothing in the officials' manner of presentation that renders the procedure surrounding the array suggestive, the principal question is whether the picture of the accused, which matches descriptions given by the witness, so stood out from all of the other photographs as to 'suggest to an identifying witness that [that person] was more likely to be the culprit.' 'In other words, the array must not be so limited that the defendant is the only one to match the witness's description of the perpetrator.
>
> The police do not have to provide a photo array containing only "exact replicas" of the defendant's picture; all that is required is that the "photos are matched by race, approximate age, facial hair, and a number of other characteristics." Thus, a photo array in which the individual characteristics of the accused, such as race, stand in stark

> contrast to the other photographs is impermissibly suggestive. [S]imply being of a different race or ethnic group from others placed in a lineup does not necessarily make the lineup impermissibly suggestive, especially where . . . the other individuals had roughly the same characteristics and features of the accused.[231]

Suggestiveness is very difficult to avoid in witness identification. If a prosecutor asks for witness identification in court without having done anything to prepare the witness,[232] the mere fact that the defendant is sitting in the defendant's place at the defense table is highly suggestive. If, on the other hand, as a prudent prosecutor would do, the witness has been prepared by a lineup, show up, or photo array, the faces included in the lineup, photo array, or show up may be suggestive under any one of a nearly endless number of theories.

If the witnesses told investigators that the perpetrator had a beard and only one person with a beard is included in the lineup, show up, or photo array, that suggests that the one with the beard is the perpetrator. On the other hand, if everyone in the lineup, show up, or photo array wears a beard, that is suggestive that being bearded is an indication of guilt.

While suggestiveness could be eliminated in theory by assuring that all the candidate images look exactly the same, or as close to that as possible, that would defeat the effort to obtain witness identification. To be sure, the defense might like such a result, because it would show that any effort to single out the defendant is unreliable since so many other people look like him.

The likelihood of a reliable identification in a lineup, show up, or photo array is increased in proportion to the number of candidate images included; if a witness is shown only two faces, the implication is strong that the perpetrator is one of the two, creating a 50-50 chance of misidentification, if the witness is uncertain. To have integrity, all of these out of court procedures must allow for the possibility that the face of the perpetrator is not included.

Three traditional techniques for pre-trial witness identification are common: lineups, show ups, and photo arrays. In a lineup, multiple individuals are presented to the witness at the same time, and the witness is asked to pick out the perpetrator. In a show up, one individual is presented to the witness, and the witness is asked if that individual is the

---

231. *Id.* at 191–92 (all alterations except the first in original, internal quotations and citations omitted).

232. For a prosecutor to do this, the prosecutor must have extremely low risk aversion; the risk is enormous that the witness may not make a convincing identification. This conclusion flows from the author’s experience with the importance of preparation for trial.

perpetrator.[233] A photo array is similar to a lineup in that multiple subjects are presented to the witness, but they are presented through photographs rather than being physically present.

In *Williams v. Bauman*,[234] the court of appeals summarized the constitutional limitations on lineup identification:

> [U]se by the police of an identification procedure may at times pose due process concerns—but it does so "only when law enforcement officers use an identification procedure that is both suggestive and unnecessary." *Perry v. New Hampshire*, —— U.S. ——, 132 S. Ct. 716, 724 (2012). Even then, suppression of the evidence is warranted only if, on the totality of the circumstances, "improper police conduct created a 'substantial likelihood of misidentification." *Id.* (quoting *Neil v. Biggers*, 409 U.S. 188, 201, 93 (1972)). "The 'corrupting effect of the suggestive identification' must be weighed against factors indicating that the eyewitness identification is reliable, including "the opportunity of the witness to view the criminal at the time of the crime, the witness' degree of attention, the accuracy of his prior description of the criminal, the level of certainty demonstrated at the confrontation, and the time between the crime and the confrontation." *Manson v. Brathwaite*, 432 U.S. 98, 114 (1977).[235]

Footnote 26 in *Wade* quoted a law review article proposal for safeguarding the reliability of lineups:

> - Give suspects the right to counsel during any lineup or during any confrontation.
> - Require that a victim or witness give a description of the suspect before viewing any arrested person. A written record of this description would be required, and the witness would have to sign it.
> - Make available any record of a suspect's description to defense counsel for use in testing the accuracy of the identifications made during the lineup and during the trial.
> - Requirement for at least six persons in addition to the accused in a lineup, and these persons would have to be of approximately the same height, weight,

233. *E.g.*, *What Are the Rules for Police Lineups?*, *supra* note 33 (defining lineups and show ups).

234. Williams v. Bauman, 759 F.3d 630, 638 (6th Cir. 2014).

235. *Id.* at 638–39.

coloration of hair and skin, and bodily types as the suspect.

- Requirement that all subjects be dressed alike. If distinctive garb was used during the crime, the suspect should not be forced to wear similar clothing in the lineup unless all the other persons are similarly garbed.
- Complete written report of the names, addresses, descriptive details of the other persons in the lineup, and of everything which transpired during the identification.
- Limiting voice identification tests by having each person in the lineup repeat identical innocuous phrases, and it would be impermissible to force the use of words allegedly used during a criminal act.
- Prohibiting the police from suggesting to any viewer that one or more persons in the lineup had been arrested as a suspect.
- Requiring multiple witnesses making an identification, to do so separately and be forbidden to speak to another witness until all of them have completed the process.
- Requiring the use of movie cameras and tape recorders to record the lineup process in those states which are financially able to afford these devices.
- Exclude evidence obtained as the result of a violation of these requirements.[236]

In *Perry v. New Hampshire*,[237] the Supreme Court rejected an argument that a show up violated due process. Although the defendant was standing next to a police officer in an apartment parking lot, the witness spontaneously looked out her window and identified him as the person she saw preparing to break into cars. The police did not arrange for her to look at the defendant or tell her to look out the window of her apartment at the parking lot. They simply asked her if she could identify the person she had seen. The Court held that the Due Process Clause did not come into play because there was no state action; the police did not arrange the show up. Thus, the evidence was admissible, even though the witness was unable to identify the defendant later from a photo array.

---

236. United States v. Wade, 388 U.S. 218, 236 n.26 (1967) (quoting Murray, *The Criminal Lineup at Home and Abroad*, 1966 UTAH L. REV. 610, 627–28).

237. Perry v. New Hampshire, 565 U.S. 228 (2012).

The Court characterized several kinds of suggestive identification that are constitutionally suspect, specifically:

> [p]olice-designed lineups where "all in the lineup but the suspect were known to the identifying witness, . . . the other participants in [the] lineup were grossly dissimilar in appearance to the suspect, . . . only the suspect was required to wear distinctive clothing which the culprit allegedly wore, . . . the witness is told by the police that they have caught the culprit after which the defendant is brought before the witness alone or is viewed in jail, . . . the suspect is pointed out before or during a lineup, . . . the participants in the lineup are asked to try on an article of clothing which fits only the suspect."[238]

In *Simmons v. United States*,[239] the Supreme Court explained how the reliability of in-court identification can be undermined by the procedures used to present photo arrays:

> It must be recognized that improper employment of photographs by police may sometimes cause witnesses to err in identifying criminals. A witness may have obtained only a brief glimpse of a criminal, or may have seen him under poor conditions. Even if the police subsequently follow the most correct photographic identification procedures and show him the pictures of a number of individuals without indicating whom they suspect, there is some danger that the witness may make an incorrect identification. This danger will be increased if the police display to the witness only the picture of a single individual who generally resembles the person he saw, or if they show him the pictures of several persons among which the photograph of a single such individual recurs or is in some way emphasized. The chance of misidentification is also heightened if the police indicate to the witness that they have other evidence that one of the persons pictured committed the crime. Regardless of how the initial misidentification comes about, the witness thereafter is apt to retain in his memory the image of the photograph rather than of the person actually seen, reducing the trustworthiness of subsequent lineup or courtroom identification.[240]

---

238. *Id.* at 243 (quoting *Wade*, 388 U.S. at 233).

239. Simmons v. United States, 390 U.S. 377 (1968).

240. *Id.* at 383–84 (footnotes omitted) (rejecting challenge to identification based on a photo array).

The same logic for photo arrays applies to show ups and lineups. In *United States v. Hargrove*,[241] the court of appeals rejected a post-conviction claim that eyewitness identifications made from a photo array were unduly suggestive.

> Hargrove contends that because he was the only officer depicted in the photo array with a beard and glasses, his photo stood out from the others to such a significant extent that witnesses were predisposed to select it over the others. We disagree. First, his photo does not stand in such stark contrast to the others in the array, which all depict black CPD officers of similar age with short hair and some degree of facial hair. Second, the glasses and beard were not suggestive of anything given that none of the Alsip officers had told investigators that any of the four men at the apartment were bearded or wore glasses. *See United States v. Moore*, 115 F.3d 1348, 1360 (7th Cir.1997) (rejecting a claim that a photo array was unduly suggestive because the defendant was the only person depicted with a 'notched eyebrow' because only one of several eyewitnesses had described the suspect as having a distinctive eyebrow); *United States v. Gibson*, 135 F.3d 257, 260 (2d Cir.1998) ("[B]ecause [the defendant] did not establish that [the eyewitness] told police the perpetrator wore a goatee, portraying [the defendant] with a goatee would not be suggestive."). Accordingly, the photo array was not unduly suggestive, and it was not error to admit the Alsip police officers' identifications of Hargrove.[242]

In *United States v. Clayborne*,[243] the district court thoroughly reviewed arguments of suggestiveness of a photo array, including academic studies and the "Yates Memorandum," and rejected all of them.[244]

Williams, *Perry*, *Bernal*, and the other cases cited in this Section articulate the appropriate legal framework for evaluating witness identifications that begin with computerized face-matches. The defendant should be able to question the reliability of the identification by scrutinizing, through cross examination, how the face-recognition system produced the image or images presented to the witness. If only one image is presented, and the witness is told it is the image selected by a computer as being the image of the perpetrator, the virtual show up is ipso facto

241. United States v. Hargrove, 508 F.3d 445 (7th Cir. 2007).

242. *Id.* at 450–51.

243. United States v. Clayborne, 425 F. Supp. 3d 1047, 1048 (E.D. Wis. 2019) (denying motion to suppress witness identification).

244. *Id.* at 1052–62.

suggestive. Whether the witness adds any significant independent corroboration is questionable. Reliability of the identification depends entirely on the reliability of the software and its algorithms. Even if the witness is not told that the single image was produced by a face-matching program, presentation of a single image is inherently suggestive.

On the other hand, if the witness is shown multiple faces generated by the computer system, they will resemble each other (if the face-matching system is any good at all), and the suggestiveness sometimes present in a conventional lineup photo array is reduced.

In the computer face-matching context, if the witness is shown one facial image and told that the computerized face-matching program picked that one out, the suggestiveness is obvious. That is worse than if the witness is shown the single image without being told how it was selected. Likewise, if the witness is shown five faces, and told that a particular one is the product of a computerized face-match, the suggestiveness is similarly high.

If, as is more likely, the witnesses are shown five or ten faces and told the computer program selected all of them were selected by the computer program as possible matches, the implication is strong that one of the arrays must be the perpetrator.

If, on the other hand, a computerized matching program is used to select one or more of the images presented to the witness, and the witness is not told that any of them came from the system, use of the technology has not contributed to suggestiveness. Indeed, if a computerized program has any statistically significant reliability at all, the likelihood of accurate identification has been increased materially.

The holding in *Wade* suggests one approach to enhance the reliability of computerized face-matching: allow the defendant's counsel to participate in the computer run that results in face-matches. Of course, some that adaptation of this basic principle would be necessary. Before running the face-match program, investigators do not know who the suspect is, and therefore cannot identify a suspect's lawyer, even if he has one at that point. So, the program could be run and then those resultant suspects who survive post-match screening would be notified that they are targets of an investigation. They would be entitled to have their counsel scrutinize the results of the face-matching process, perhaps involving no more than disclosure of the fact that it was done.

Mere disclosure might not do defense counsel much good, however, unless the scope of criminal discovery entitled him to obtain more information about the face-matching algorithm and how it was used or unless the operation of the face-matching algorithm was fair subject matter for cross examination at trial.

2. Adjudicating Suggestiveness

Evaluating suggestiveness requires defense counsel access to the procedures that may have been suggestive. This can begin with defendant representation by counsel at lineups, show ups, or photo arrays under *Wade*. But many such procedures occur before a defendant is identified as a suspect; indeed, their purpose is to identify suspects. No counsel is going to be present under *Wade* in such circumstances. In light of this, the important questions are: (1) whether the defendant is entitled to a pre-trial hearing on a motion to exclude eyewitness identification because it has been tainted by identification procedures; and (2) whether the details of the identification procedures are admissible into evidence if the testimony is allowed.

The law is reluctant to approve sideshows unnecessarily litigating the details of investigatory procedures that, in the end, did not matter.[245] In *People v. Wharton*,[246] the New York Court of Appeals held that a "*Wade* hearing" was unnecessary, because the identification was made by a skilled law enforcement officer shortly after the time of the crime. Improper suggestiveness was unlikely.[247]

Some courts use the term "*Wade* hearing" more narrowly than others. To some, it refers to a hearing to determine whether a defendant had a right to counsel at a pre-trial identification procedure. Others, probably the majority, use the term to refer to any hearing of the admissibility of possible suggestive pre-trial identifications.

State v. Henderson[248] is, perhaps, an extreme example of an elaborate pre-trial procedure. There, the New Jersey Supreme Court appointed a special master to evaluate the reliability of eyewitness identifications. The special master heard testimony by seven experts and produced more than 2,000 pages of transcripts and hundreds of scientific studies.[249] The resulting decision overruled earlier caselaw and overhauled New Jersey law on witness identification.

> When defendants can show some evidence of suggestiveness, all relevant system and estimator variables should be explored at pre-trial hearings. A trial court can end the hearing at any time, however, if the court concludes from the testimony that defendant's threshold allegation of

245. *See* State v. Henderson, 27 A.3d 873, 924–25 (N.J. 2011) (expressing concern about adverse effect on judicial resources of allowing pre-trial hearings in too many cases; unreliability arising from estimator variable more appropriately addressed by cross examination and jury instructions).

246. People v. Wharton, 549 N.E.2d 462, 462 (N.Y. 1989) (affirming conviction).

247. *Id.* at 463.

248. 27 A.3d 872 (N.J. 2011).

249. *Id.* at 877.

> suggestiveness is groundless. Otherwise, the trial judge should weigh both sets of variables to decide if the evidence is admissible.[250]

The court gave examples of the kinds of proffers that should lead to "*Wade* hearings."[251]

In *Henderson*,[252] the New Jersey supreme court specified the order of proof to enable a court to decide whether to exclude eyewitness identification testimony. In doing so, it suggested nine "system-variable" questions and thirteen "estimator" questions to decide a motion to exclude.[253] The same questions provide a useful template for questions at trial intended to impeach eyewitness identification that is admitted. In other words, all is not lost if a "*Wade* hearing" is unavailable. The challenges that would have been made at the "*Wade* hearing" can and should be made in cross examination at trial.

In declining to mandate pre-trial review of suggestive identifications not arranged by the police, as a matter of Sixth Amendment law, the *Perry* Court pointed to other protections against erroneous eyewitness identifications:

> These protections include the defendant's Sixth Amendment right to confront the eyewitness. See *Maryland v. Craig*, 497 U.S. 836, 845 (1990) ("The central concern of the Confrontation Clause is to ensure the reliability of the evidence against a criminal defendant."). Another is the defendant's right to the effective assistance of an attorney, who can expose the flaws in the eyewitness' testimony during cross examination and focus the jury's attention on the fallibility of such testimony during opening and closing arguments. Eyewitness-specific jury instructions, which many federal and state courts have adopted, likewise warn the jury to take care in appraising identification evidence. *See, e.g., United States v. Telfaire*, 469 F.2d 552, 558–59 (C.A.D.C. 1972) *(per curiam)* (D.C. Circuit Model Jury Instructions) ("If the identification by the witness may have been influenced by the circumstances under which the defendant was presented to him for identification, you should scrutinize the identification with great care."). See also *Ventris*, 556 U.S., at 594, n.* (citing jury instructions that informed jurors about the unreliability of uncorroborated jailhouse-informant testimony as a reason to

250. *Id.* at 878.

251. *See id.* at 921–23 (offering examples of proffers that would warrant a *Wade* hearing).

252. 27 A.3d 872 (N.J. 2011).

253. *Id.* at 920–22; *see id.* at 896–910 (identifying eight "system" variables under the control of investigators and ten "estimator" variables outside their control to be considered in evaluating reliability of witness identification based on lineups, showups, and photo arrays).

> resist a ban on such testimony); *Dowling*, 493 U.S., at 352–53. The constitutional requirement that the government prove the defendant's guilt beyond a reasonable doubt also impedes convictions based on dubious identification evidence.
>
> State and Federal Rules of Evidence, moreover, permit trial judges to exclude relevant evidence if its probative value is substantially outweighed by its prejudicial impact or potential for misleading the jury. *See, e.g.*, Fed. Rule Evid. 403; N.H. Rule Evid. 403 (2011). See also Tr. of Oral Arg. 19–22 (inquiring whether the standard Perry seeks differs materially from the one set out in Rule 403). In appropriate cases, some States also permit defendants to present expert testimony on the hazards of eyewitness identification evidence. *See, e.g.*, *State v. Clopten*, 2009 UT 84, ¶ 33, 223 P.3d 1103, 1113 ("We expect ... that in cases involving eyewitness identification of strangers or near-strangers, trial courts will routinely admit expert testimony [on the dangers of such evidence].").[254]

The opportunity to cross examine based on pre-trial identification procedures or to exclude trial testimony based on those procedures depends on the defendant's knowing about the procedures. In New York, a statute requires the state to give pre-trial notice to the defendant of its intent to introduce eyewitness identification.[255] After receiving such notice, the defendant may request a "*Wade* hearing."[256]

Other discovery rules extend discovery to pre-trial tests and experiments in a way that would include computerized face-matching runs. The federal discovery rules require the government to disclose to the defendant the results "of any scientific test or experiment" if the "material is material to preparing the defense or the government intends to use the item in its case-in-chief."[257] The 1966 Advisory Committee notes say that "scientific tests or experiments" include fingerprint and handwriting comparisons.

---

254. Perry v. New Hampshire, 565 U.S. 228, 245–47 (2012).

255. N.Y. C.P.L.R. 710.30(1) (McKinney 2019) (governing "testimony regarding an observation of the defendant either at the time or place of the commission of the offense or upon some other occasion relevant to the case, to be given by a witness who has previously identified him or her or a pictorial, photographic, electronic, filmed or video recorded reproduction of him or her as such").

256. N.Y. C.P.L.R. 710.30(2) (McKinney 2019); *see* People v. Boyer, 846 N.E.3d 461, 463 (N.Y. 2006) (describing and applying CPL 710.30; reversing conviction for failure to afford a Wade hearing).

257. FED. R. CRIM. P. 16(a)(1)(F).

ABA Criminal Justice Standards for Discovery require the prosecution to disclose to the defense, "[a]ny material, documents, or information relating to lineups, show ups, and picture or voice identifications in relation to the case."[258]

The recently revised Virginia criminal discovery rules entitle a defendant to obtain, on motion:

> written reports of autopsy examinations, ballistic tests, fingerprint analyses, handwriting analyses, blood, urine and breath tests, other scientific reports, and written reports of a physical or mental examination of the accused or the alleged victim made in connection with the particular case, that are known by the Commonwealth's attorney to be within the possession, custody, or control of the Commonwealth.[259]

The results of a computerized face-matching run would qualify as an "other scientific report," and it would have been run "in connection with the particular case," so a Virginia defendant can obtain this material.

3. Wanted Posters

Computerized face-recognition systems can be used to create wanted posters—either of the conventional paper design or in a digital form, posted on the Internet. Wanted posters sometimes raise issues as to whether they are a sufficient basis for probable cause for an arrest or reasonable suspicion for a *Terry*[260] stop.

In *United States v. Hensley*,[261] the Supreme Court concluded that:

> if a flyer or bulletin has been issued on the basis of articulable facts supporting a reasonable suspicion that the wanted person has committed an offense, then reliance on that flyer or bulletin justifies a stop to check identification, to pose questions to the person, or to detain the person briefly while attempting to obtain further information.[262]

---

258. STANDARDS FOR CRIMINAL JUSTICE: DISCOVERY AND TRIAL BY JURY, 11–2.1(a)(vii) (AM. BAR ASS'N 1996), https://www.americanbar.org/content/dam/aba/publications/criminal_justice_standards/discovery_trialbyjury.pdf.

259. VA. R. CRIM. P. 3A:11(b)(2)(D).

260. Terry v. Ohio, 392 U.S. 1, 20–22 (1968) (holding that an investigatory "stop and frisk" is a Fourth Amendment seizure and search but does not require the probable cause necessary for an arrest; specific and articulable facts giving rise to reasonable suspicion suffice).

261. 469 U.S. 221 (1985).

262. *Id.* at 232 (1985) (citation omitted); *see also* Beaver, *supra* note 26 ("If there is a wanted poster issued, as opposed to a person of interest poster, it is highly likely there is also a warrant issued by a judge, which should give law enforcement the authority to at least detain and identify someone reasonably thought to be the person.").

The Court reviewed the record and concluded that specific and articulable facts supported issuance of the wanted poster.[263]

In the face-recognition context, the outcome-determinative question would be whether the generation of a matching image constitutes "specific and articulable facts" justifying the content of a wanted poster. The most permissive possibility is that the mere existence of the computerized match satisfies the test. A more restrictive possibility is that the standard must be tested by evidence about the reliability of the probe image, the appropriateness of the enrolled database, and the robustness of the face-matching algorithms.

F. *Challenging Scientific Methods of Identification and the Experts Presenting Them*

Case law involving fingerprint and DNA evidence helps frame the analysis of computerized face matching differently from conventional witness identification. While the suggestiveness concepts analyzed in the preceding two Sections provide support for the defendant's right to access to pre-trial computer face-identification procedures, it offers only partial guidance as to the content of the challenge, once access is available. As those Sections explain, suggestiveness can be adapted to a case in which in court witness identification is central to the prosecution's theory. The fingerprint and DNA law gives more guidance as to exactly what can and should be probed in terms of the science and the implementation of the scientific identification procedures.

1. Expert Witnesses

Fingerprint and DNA identification cases provide the guide for the use of expert testimony to present computerized face-matching evidence or to defend its use with witnesses in the pre-trial context.

One district court explained the order of proof:

> Before a witness may testify as an expert, a district court must make three express findings. First, the court must find that the proposed witness is qualified to offer expert testimony. Second, the court must find that the witness has applied reliable principles. Third, the court must find that the witness's testimony may help the jury understand evidence or determine a fact at issue in the case. So long as an expert meets these threshold considerations, the expert may testify; it is up to the jury to determine the weight to give that testimony. Shaky but admissible evidence is to be attacked by cross examination, contrary evidence, and attention to the

263. *Hensley*, 469 U.S. at 233–34.

> burden of proof, not exclusion. The proponent of the expert testimony bears the burden of establishing its admissibility by a preponderance of the evidence.[264]

2. Voir Dire

The first step in introducing scientific evidence through expert testimony is to establish the expert's qualifications. In *Mulder v. State*, for example, the Nevada Supreme Court held that a witness offered by the defense did not qualify as an expert.[265] During the prosecutor's voir dire examination, Doulder revealed that the IAI listed him as an expert in questioned documents, not fingerprints. Doulder was listed as an IAI fingerprint expert in 1950; although he is no longer listed, he testified, "Fingerprints haven't changed from 1950 to now. They are the same." Additionally, the prosecutor elicited testimony that although Doulder had testified about fingerprinting in recent trials in Las Vegas, the presiding judges in those trials refused to determine that he was a qualified fingerprint expert. Doulder admitted that ninety percent of his work is in questioned documents and only ten percent deals with fingerprints.[266]

3. Admissibility of Science

Scientific opinion testimony is not admissible unless it meets the tests of *Frye*[267] or *Daubert*.[268]

In *Allen v. State*,[269] the court reversed a conviction for sexual battery, kidnapping, and burglary, because expert testimony on DNA evidence was wrongfully admitted. The witness had ten-years' experience in the field of DNA analysis, had testified as an expert more than two dozen times, and had a master's degree in pharmaceutical science with an emphasis in forensics DNA and serology.[270] She did not, however, demonstrate expertise in statistical probability.[271] Defense counsel properly objected on the grounds that the witness had "not been qualified

---

264. United States v. Wells, No. 3:13-CR-00008-SLG, 2019 WL 3229912, at *1 (D. Alaska July 17, 2019) (internal quotations and footnotes omitted).

265. Mulder v. State, 992 P.2d 845, 853 (Nev. 2000).

266. *Id.* at 852.

267. *See* Savage v. State, 166 A.3d 183, 194 (Md. 2017) ("The standard enunciated in Frye v. United States, 293 F. 1013 (D.C. Cir. 1923) . . . makes evidence emanating from a novel scientific process inadmissible absent a finding that the process is generally accepted by the relevant scientific community.").

268. *See id.* at 204 (discussing that the *Daubert* standard probes beneath scientific acceptability and examines reliability and validity); *id.* at 205–07 (Adkins, J., concurring) (arguing that Maryland should explicitly adopt the standard of Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579 (1993), rather than *Frye*).

269. 62 So. 3d 1199 (Fla. Dist. Ct. App. 2011).

270. *Id.* at 1200.

271. *Id.* at 1200–01.

as an expert in statistical probability." At this point, it was the state's burden to prove that the expert was qualified, and not Allen's burden to show that she was not. *See Brim v. State*, 695 So.2d 268, 272 (Fla.1997); *Hudson v. State*, 844 So.2d 762, 763 (Fla. 5th DCA 2003) ("[T]he state must prove by a preponderance of evidence that an expert testifying about DNA statistical and population genetics analysis must demonstrate 'sufficient knowledge of the database grounded in the study of authoritative sources." (quoting *Murray*, 692 So.2d at 164)).

Because the record does not reveal the statistical methodology used to calculate the DNA population frequencies in this case, or Ms. Whitten's qualifications to present this evidence, we reverse Allen's conviction and sentence and remand this case to the trial court for a limited evidentiary hearing similar to the ones ordered in *Gibson* and *Miles*. On remand, the trial court is to (1) assess Ms. Whitten's competence to present the statistical evidence; and (2) clarify the exact methodology and database used for her calculations. If requested and depending on the methodology and database used, the trial court should also conduct a *Frye* hearing to determine the general acceptance of the employed statistical techniques and database. *See Roberts v. State*, 841 So.2d 558, 560 (Fla. 4th DCA 2003). If following a hearing, the court determines that there was a sufficient basis for admitting the DNA evidence presented at trial, the court should reinstate the conviction and sentence. If the court determines, however, that the DNA evidence was not presented by a qualified witness, then it should grant a new trial.[272]

4. Specific Challenges to Comparisons

Reception of computerized face-matching evidence can benefit from following principles developed for fingerprint-matching evidence. Fingerprints have been around much longer than DNA or computerized face-recognition as a form of evidence. Validation of fingerprints confronted courts long before digital computers. The criminal justice system established the need for a certain number of landmarks to validate a fingerprint comparison. Now that computerized fingerprint comparison is feasible and in common use,[273] the same determinants of reliability should be subject to probing cross examination. It should not matter that the computer has identified a "whorl" rather than a human expert doing it. The factfinder needs to know how the computer program went about

272. *Id.* at 1202.

273. *See* Maryland v. King, 569 U.S. 435, 459 (describing FBI's IAFIS, its computerized fingerprint analysis tool, launched in 1999); *see also* ARUN ROSS ET AL., *A Hybrid Fingerprint Matcher*, 36 Pattern Recognition 1661 (2003), http://biometrics.cse.msu.edu/Publications/Fingerprint/RossJainReisman_HybridFpMatcher_PR03.pdf [https://perma.cc/UFN6-3EX2] (explaining system for one-to-many fingerprint matching).

identifying that artifact of the fingerprint.[274] This is especially important, given the limitations of automated fingerprint matching systems.[275] Automated fingerprint matching produces the same kinds of results as computerized face-matching. It outputs some potential matches with an assessment of probabilities of actual match.[276] Traditional automated fingerprint matching uses only ridges on fingerprints.[277] The research frontier is to automate searching based on fingerprint minutiae as well. That kind of composite matching would significantly improve accuracy.[278]

The Illinois intermediate court explained how automated fingerprint searching and matching works in *People v. Slover*:[279]

> A fingerprint examiner conducting an AFIS search on a latent print scans an image or a tracing of the print into the computer; isolates its high-quality area; pinpoints its "core"; orients it along a vertical "axis"; locates the "points," or "points of minutiae," or "points of comparison"—areas where a ridge ends or bifurcates; identifies the print's pattern type; and identifies, if possible, which finger on which hand made the print. Computers are unable to identify the core, axis, points, pattern type, and finger; an examiner must provide this information to the computer executing the search. Identifying the pattern type and finger narrows the scope of the search so only a corresponding subset of AFIS's 60 million prints is searched. AFIS employs an algorithm or algorithms selected by the examiner to compare the latent fingerprint to those stored in its database based on the relative locations of the core, axis, and points. It assigns a score to each searched print reflecting the relative likelihood

274. *See* Moses, *supra* note 29, at 6-25 to -26 (describing algorithms for ridge identification and minutiae extraction); *see also Transcript of Direct and Cross Examination of William Reeves* (2007), http://defensewiki.ibj.org/images/a/ac/Reeves_William_Fingerprints_2007_01_9_amp_10_Dowdy.pdf [https://perma.cc/AJN8-GM96] (transcript of direct and cross examination of fingerprint expert).

275. *See* Anil K. Jain et al., *Biometrics: Fingerprint Matching*, COMPUTER, at 36, 44 (Feb. 2010), *available at* http://biometrics.cse.msu.edu/Publications/Fingerprint/JainFpMatching_IEEEComp10.pdf [https://perma.cc/D43G-MWAN] (summarizing limitations of automated fingerprint matching systems; human experts still outperform them); Moses, *supra* note 29, at 6-11 (assessing accuracy of AFIS as 70–80%).

276. *See Automated Fingerprint Identification System (AFIS)*, TEX. DEP'T PUB. SAFETY, https://www.dps.texas.gov/CrimeLaboratory/AFIS.htm [https://perma.cc/V4FT-KPLM] (last visited Jan. 11, 2021) (describing how AFIS finds "closest matching prints" and provides list to human examiner).

277. *Id.* (describing submission of ridge information to system).

278. Moses, *supra* note 29, at 6-27 to -28 (explaining why human experts are, so far, better than automated fingerprint matching systems).

279. 959 N.E.2d 72, 73–74 (Ill. App. Ct. 2011).

> of matching it to the latent print. No matter the quality or quantity of the information submitted or the likelihood of obtaining a match, AFIS provides a list of the 10 highest scoring stored fingerprints, along with a computer image of each print and identifying information on the person to whom the print belongs, such as his or her name, sex, race, and age. The examiner compares computer printouts of the 10 potential matches to the latent print to determine whether any of the stored prints can be positively eliminated as a match; if a print cannot be eliminated as a possible match, then the examiner requests its original to be sent from a central facility for further comparison.[280]

Conflicting testimony about the results obtainable from a set of latent fingerprints caused the court to deny a motion for further testing:

> [T]he trial court heard testimony by the State's and defendants' experts debating the "suitability" of the guardrail fingerprint for AFIS testing. Kenneth Moses, an expert for defendants, was director of Forensic Identification Services, an independent forensics laboratory in San Francisco. Moses testified he studied the ISP's standards for AFIS comparison of latent fingerprints and concluded the guardrail print was suitable to be run through AFIS. He opined the print came from the upper part of a thumb. From an image of the print provided to him by defendants, Moses identified 13 points—the ISP's guidelines recommend that a minimum of 8 be identified. Although the core was not visible in the available portion of the print, Moses recommended running the print through AFIS two or three times with different estimations of the core's location and the axis's orientation. These estimations would be "a lot more than guess[es]" as they would reflect Moses's experience examining thousands of fingerprints.
>
> Mary McCarthy, the State's expert, was the latent print training coordinator for the ISP. She testified she determined the guardrail print was unsuitable for AFIS testing. She could definitively identify only about six points on the print. Other possible points were unclear or obscured and would have been cropped out if she were going to search for the print in AFIS. Further, some points seemed so high up on the finger that, McCarthy opined, they were unlikely to be included in any fingerprint stored in AFIS's database. She explained stored fingerprints often omit the fingertip due to the finger's curvature. McCarthy testified she was unable to determine the core's location and the axis's orientation and

280. *Id.*

> to identify the pattern type. Her training taught her not to guess the location of points or the core, the orientation of the axis, or the pattern type. McCarthy explained latent fingerprints with no identifiable pattern type should not be searched in AFIS. She testified Moses's proposed method of conducting multiple searches using different estimations of the core and axis was contrary to her training.[281]

This controversy over computerized fingerprint matching suggests one approach for challenging computerized face-matching. The challenger would focus on the probe image, the analogue of the guardrail print in *Slover*. A challenge based on a relatively small number of discernable features in the probe image is analogous to the claim that the number of points in the guardrail fingerprint was inadequate.

In *United States v. Rivas*,[282] the court of appeals described expert testimony and cross examination with respect to a fingerprint match:

> Rottman had been working as a forensic scientist for the Illinois State Police for approximately twenty-three years at the time of trial and had identified persons through fingerprint comparison tens of thousands of times. He explained that he compares fingerprints using the ACE-V side-by-side comparison technique. ("ACE-V" is an acronym for Analysis, Comparison, Evaluation, and Verification and is "the standard method for determining whether two fingerprints are from the same person." *United States v. Herrera*, 704 F.3d 480, 484 (7th Cir. 2013) (describing method in detail); *see also United States v. Saunders*, 2016 WL 3213039, at *5 (7th Cir. 2016)).
>
> Rottman explained that when comparing prints, he places the latent (unidentified) print next to a known print. Looking through a magnifying glass, he looks at the latent print for a point or group of points that stand out and then looks to see whether the same point or points are present in the known print. Rottman continues to look back and forth between the two prints, identifying individual points or characteristics as well as the overall flow of the ridges and pattern and shapes, until he arrives at a conclusion. After this explanation, the government asked that Rottman be permitted to offer expert testimony pursuant to Federal Rule of Evidence 702 in the area of fingerprints and fingerprint evidence. The defense responded that it had no objection other than to make the testimony subject to cross examination.
>
> Specific to Rivas's case, Rottman testified that he developed a latent partial print from the 9 millimeter

281. *Id.* at 74.

282. 831 F.3d 931 (7th Cir. 2016).

> handgun found in the storage unit, photographed the print, and then lifted it. He then conducted a side-by-side, ACE-V comparison of the latent print to a known partial fingerprint of Rivas. After doing so, Rottman concluded that the latent partial print on the gun belonged to Rivas. Rottman showed the jury images of both the latent and known prints and walked the jury through ten points of comparison. He testified that he had found seventeen points of comparison between the latent and known partial prints and that they made him "totally certain" that the partial print on the gun was from Rivas.
>
> The defense cross examined Rottman regarding his development of the partial fingerprint from the gun and also about his side-by-side comparison. During the cross examination, Rottman acknowledged the conclusion of a 2009 National Academy of Sciences report published by the National Research Council that it was not possible to have a zero error rate in fingerprint analysis. Rottman further acknowledged that he was not aware of any studies validating the reliability of the ACE-V method. The defense also attempted to cross examine Rottman regarding a different fingerprint examiner's conclusion in a separate case, that of Brandon Mayfield. The government objected, and the trial court sustained the objection. As a result, Rivas was not allowed to introduce evidence of Mayfield's erroneous identification through the ACE-V method of fingerprint analysis.[283]

The court rejected the argument that limiting the cross examination violated the Sixth Amendment. The witness was not involved in the other, erroneous, identification.[284]

Rivas suggests the importance of being able to access and thus being able to cross examine based on the details of the process used for comparison, whether human or computerized.

In *Narrod v. Napoli*,[285] the district court denied a habeas petition alleging unconstitutional limitation on cross examination of a fingerprint expert. The court quoted the prosecution's acknowledgment of the limitations of automated fingerprint matching:

> The prosecutor objected, stating that SAFIS "has never passed a Frye test in terms of being admissible in court," that there was no foundation for the testimony, and that "SAFIS is a tool that's used to give fingerprint examiners possible

283. *Id*. at 933–34.

284. *Id*. at 935.

285. 763 F. Supp. 2d 359 (W.D.N.Y. 2011).

> prints to then make a comparison from. It is not a tool that's used to make identifications. It's just simply not reliable. We [the prosecution] can never come into court and say, oh, this is his fingerprint based on results from SAFIS."[286]

The current state of the art for computerized face-matching is like the state of the art for AFIS. Proponents of computerized face-matching use it as an intermediate step for witness identification, just like proponents of automated fingerprint matching use it as a shortcut for further analysis of fingerprints by human experts. That does not mean, however, that the involvement of computerized face-matching is inadmissible in the cross examination of a human who has seen the computer-generated results. The possibility of suggestiveness exists, whether the comparison involves fingerprints or faces.

5. The Less Human Involvement, the Greater the Reliability?

Judge Posner, in *United States v. Herrera*, offered a detailed explanation of fingerprint matching and compared it with DNA matching:

> Visual comparison consists of discerning, visually "measuring," and comparing—within the comparable areas of the latent print and the known prints—the details that correspond. The amount of friction ridge detail available for this step depends on the clarity of the two impressions. The details observed might include the overall shape of the latent print, anatomical aspects, ridge flows, ridge counts, shape of the core, delta location and shape, lengths of the ridges, minutia location and type, thickness of the ridges and furrows, shapes of the ridges, pore position, crease patterns and shapes, scar shapes, and temporary feature shapes (e.g., a wart).
>
> At the completion of the comparison, the examiner performs an evaluation of the agreement of the friction ridge formations in the two prints and evaluates the sufficiency of the detail present to establish an identification (source determination). Source determination is made when the examiner concludes, based on his or her experience, that sufficient quantity and quality of friction ridge detail is in agreement between the latent print and the known print. Source exclusion is made when the process indicates sufficient disagreement between the latent print and known print. If neither an identification nor an exclusion can be reached, the result of the comparison is inconclusive. Verification occurs when another qualified examiner repeats

286. *Id.* at 379.

> the observations and comes to the same conclusion, although the second examiner may be aware of the conclusion of the first.[287]

The court compared fingerprint analysis with DNA analysis:

> The methodology requires recognizing and categorizing scores of distinctive features in the prints, see Davide Maltoni et al., *Handbook of Fingerprint Recognition* 97–101 (2d ed. 2009); Federal Bureau of Investigation, *The Science of Fingerprints: Classification and Uses* 5–86 (2006), and it is the distinctiveness of these features, rather than the ACE–V method itself, that enables expert fingerprint examiners to match fingerprints with a high degree of confidence. That's not to say that fingerprint matching (especially when it involves latent fingerprints, as in this case) is as reliable as DNA evidence, for example. Forensic DNA analysis involves comparing a strand of DNA (the genetic code) from the suspect with a strand of DNA found at the crime scene. The comparison is done with scientific instruments and determines whether the segments are chemically identical. Errors are vanishingly rare provided that the strands of code are reasonably intact. As we explained in *United States v. Ford*, 683 F.3d 761, 768 (7th Cir.2012),
>
> What is involved, very simply, in forensic DNA analysis is comparing a strand of DNA (the genetic code) from the suspect with a strand of DNA found at the crime scene. See "DNA Profiling," *Wikipedia*, http://en.wikipedia.org/wiki/DNA_profiling [https://perma.cc/9VZV-E7MV] (visited May 31, 2012). Comparisons are made at various locations on each strand. At each location there is an allele (a unique gene form). In one location, for example, the probability of a person's having a particular allele might be 7 percent, and in another 10 percent. Suppose that the suspect's DNA and the DNA at the crime scene contained the same alleles at each of the two locations. The probability that the DNA was someone else's would be 7 percent if the comparison were confined to the first location, but only .7 percent (7 percent of 10 percent) if the comparison were expanded to two locations, because the probabilities are independent. Suppose identical alleles were found at 10 locations, which is what happened in this case; the probability that two persons would have so many identical alleles, a probability that can be computed by multiplying together the probabilities of an identical allele at each location, becomes

287. United States v. Herrera, 704 F.3d 480, 484 (7th Cir. 2013) (quoting NAT'L RSCH. COUNCIL, STRENGTHENING FORENSIC SCIENCE IN THE UNITED STATES: A PATH FORWARD 137–38 (2009)).

> infinitesimally small—in fact 1 in 29 trillion, provided no other comparisons reveal that the alleles at the same location on the two strands of DNA are different. This is the same procedure used for determining the probability that a perfectly balanced coin flipped 10 times in a row will come up heads all 10 times. The probability is .510, which is less than 1 in 1000.
>
> Chemical tests can determine whether two alleles are identical, but a fingerprint analyst must visually recognize and classify the relevant details in the latent print—which is difficult if the print is incomplete or smudged. "[T]he assessment of latent prints from crime scenes is based largely on human interpretation . . . . [T]he process does not allow one to stipulate specific measurements in advance, as is done for a DNA analysis. Moreover, a small stretching of distance between two fingerprint features, or a twisting of angles, can result from either a difference between the fingers that left the prints or from distortions from the impression process." National Research Council, *supra,* at 139.[288]

His motivation for the comparison was to show that DNA evidence, though newer, and therefore potentially more controversial, is more reliable than fingerprint evidence, which depends more on human analysis. The same point can be made, based on similar comparison, between conventional eyewitness identification prompted by lineups, show ups, and photo arrays and computerized face-matching. The *Posner* analysis suggests that computerized face-matches may be more reliable than conventional pre-trial identification techniques.

In *State v. Jenkins*,[289] the court expressed doubt about the use of DNA matching to identify a defendant because of weak testimony introducing it, drawing analogies to usual examinations supporting automated fingerprint matching.

There was no testimony at trial as to who generated the Defendant's DNA profile that was uploaded into CODIS, who uploaded the Defendant's DNA into CODIS, how CODIS maintained this information, or any records concerning the use or operation of CODIS. Although the State argues it was admitted for the effect on the listener, rather than the truth of the matter asserted, there is no question that the testimony was probative of the Defendant's identity, a crucial element of the offense.[290]

Computerized DNA matching systems match only certain strands of DNA, typically those related to appearance and demographic

---

288. *Id.* at 485 (quoting NAT'L RSCH. COUNCIL, STRENGTHENING FORENSIC SCIENCE IN THE UNITED STATES: A PATH FORWARD 137–38 (2009)).

289. No. E2017-01983-CCA-R3-CD, 2018 WL 6113468 (Tenn. Ct. .App. Nov. 20, 2018).

290. *Id.* at *12.

characteristics rather than sex. That virtually all the genealogical DNA search products use autosomal testing, excluding sex chromosomes. A rich source of cross examination is to probe how the search algorithm designer selected the chromosomes to be matched, and what the implications would be if other chromosomes had been searched as well.

Scrutiny of the elements of DNA matching provides a good model for scrutiny of the elements of computerized face-matching. In particular, the Supreme Court noted the standardization of the points of comparison in DNA analysis.[291] Challenges to computerized face-matches can be based on deviation from generally accepted practice for comparison of facial features—the elements of a face vector.[292]

V. CHALLENGING COMPUTERIZED FACE-RECOGNITION EVIDENCE

This Section offers analysis of, and strategies for, dealing with hearsay and Confrontation Clause issues when face-recognition results are offered as evidence. The focus is on whether limits should be imposed on the use of face-recognition programs.

A substantial amount of literature exists about presenting and challenging fingerprint and DNA evidence. The literature includes many sample cross examination questions.[293] Section V.C adapts a set of questions from the fingerprint and DNA fields and adds to them, as appropriate, to capture the important ingredients of face—one unknown-to-many knowns—recognition technology.

A few articles exist on evidentiary issues with face-recognition.[294] They are useful starting points, but they do not go nearly far enough, focusing too much on human inputs in running the programs, and not enough on the critical design decisions that determine how the programs work.[295]

A. *Expert Testimony*

If an eyewitness identifies the defendant, expert testimony is not involved; the witness is a fact witness with personal knowledge.[296] This

---

291. Maryland v. King, 569 U.S. 435, 445 (2013) (describing CODIS, which identifies 13 loci for comparison of DNA samples).

292. *See* discussion *supra* Section II.A for an explanation of face vectors.

293. *See* Richard A. Nakashima, *DNA Evidence in Criminal Trials: A Defense Attorney's Primer*, 74 NEB. L. REV. 444, 470–72 (1995) (listing questions).

294. *E.g.*, Joseph Clarke Celentino, *Face-to-Face with Facial Recognition Evidence: Admissibility Under the Post-*Crawford *Confrontation Clause*, 114 MICH. L. REV. 1317, 1321 n.20 (2016).

295. *Id.* at 1326, 1342–44.

296. *See* FED. R. EVID. 602 (requirements for face witness testimony).

is so, even if the identification was prompted by the output of a computerized face-matching system.

If, on the other hand, testimony is offered as to the results obtained from a computerized face-matching system, expert testimony ordinarily is required. An argument is possible, however, that a lay witness is competent to testify as to routine use of a face-recognition program, and the inputs and outputs pertinent to a particular run of the program. Federal Rule of Evidence 701 allows fact-witness testimony "rationally based on the witness's perception," "not based on scientific, technical, or other specialized knowledge . . . ."[297]

When lay testimony is based on a computerized face-match, however, the same authority permitting expert testimony in "*Wade* hearings" over the suggestiveness of lineups, show ups, and photo arrays justifies allowing expert testimony on the reliability of face-matching algorithms and data.

1. Voir Dire: Qualifying Experts

The first step, according to the language quoted from Wells, is to establish the expert's qualifications. [298] When experts on computerized face-matching are proffered, two possible levels of expertise may be relevant to qualification. The less demanding level of qualification would be shown by someone with experience in using commercial face-matching products, who can testify that a particular probe image was submitted to a system, which produced certain results, in the standard way of operating the system.[299] The more demanding level of expertise would be met only by showing that the expert understood the detailed workings of the face-matching system, including the training database used to develop its algorithms, the statistical techniques used to develop its matching algorithms, the contents of the enrolled database, and how the probability assigned to possible matches were developed.[300]

Challenges and controversies depend on who gets called into court to vouch for the match resulting from use of a particular product in a

297. FED. R. EVID. 701(a) & (c).

298. United States v. Wells, No. 3:13-CR-00008-SLG, 2019 WL 3229912, at *1–2 (D. Alaska July 17, 2019).

299. Testimony to validate other types of automated systems is a useful guide. *See*, *e.g.*, People v. Rekte, 181 Cal. Rptr. 3d 912, 917–920 (Ct. App. 2015) (reviewing testimony regarding reliability of automated traffic enforcement camera).

300. "We were trained to avoid getting into these type of lines of testimony by deferring to a manufacturer because it opens you up to look stupid if you don't fully know something. For example, I could testify about how I was trained and operated equipment/software but if asked how it worked, I would refer the inquirer to whoever the manufacturer. Most of the time, attorneys won't call the manufacturer because it is expensive but if they do, the manufacturer is in the best position to defend their systems." Beaver, *supra* note 26.

particular case. A representative from the police laboratory has knowledge, and probably expertise, on how to run a particular program and the routine for maintaining the chain of custody for a particular face to be matched. Rarely, however, would such a witness know the details of the algorithms in the face-matching program. A challenger of a computerized face-match should be entitled to that information to expose the kinds of problems identified in the majority opinion in *Melendez-Diaz*[301] and by Justice Kagan's dissent in *Williams*.[302]

In *United States v. Wells*,[303] the district court considered the admissibility of expert testimony by an expert on computer forensics, video/photographic analysis, and surveillance setup. It held that the witness was qualified as an expert, because his background covered the techniques of video and photographic analysis, even though he demonstrated no particular expertise in images of automobiles, as opposed to faces, or other types of objects.[304] It also held that the expert sufficiently referenced the methods and principles on which he relied and demonstrated a rational foundation for his assertions that the government's expert evidence was flawed.[305]

2. Application of Reliable Principles: Frye or Daubert

The *Allen* case illustrates the arguments that should be made by the defendant when computerized face-matching evidence is offered. The expert vouching for the evidence must demonstrate detailed knowledge of the data used to develop the face-matching algorithms, the quality of the probe image, the contents of the enrolled database, the algorithms used to match the images, and the probability that each reported match is a good one. Given appropriate testimony about the analytical principles discussed in Section II, it should not be difficult to meet either the *Frye* or the *Daubert* standards.

3. Authentication

Federal Rule of Evidence 901(9) requires authentication of computerized face-matching evidence, by describing it and "showing that it produces an accurate result." In colloquial terms, authentication requires showing that a piece of evidence is what it purports to be. If a photograph is offered into evidence purporting to be the photograph of the perpetrator of a crime, the authentication requirement requires evidence linking the photograph to the crime. In the case of computerized

301. *See supra* text accompanying note 145.
302. *See supra* text accompanying note 166.
303. No. 3:13-cr-00008-SLG, 2019 WL 3229912 at *1 (D. Alaska July 17, 2019).
304. *Id.* at *5.
305. *Id.* at *6.

face-matching, that requires establishing: (a) the connection between the probe image and the crime scene; (b) the connection between the probe image and the reported match or matches; and (c) the connection between the reported match or matches and the defendant. Step (c) can be accomplished by the factfinder at trial. Step (a) can be established by showing that the probe photo came from surveillance video at the crime scene or by showing that the probe image was developed from witness descriptions of the perpetrator. Step (b) requires scrutiny of the face-matching databases and algorithms.[306]

In *People v. Beckley*,[307] the court rejected the admissibility of a photograph and gang roster downloaded from the Internet because the lack of authentication. The court summarized the requirement for authenticating a photograph:

> A photograph or other writing may be authenticated by the introduction of evidence sufficient to sustain a finding that it is the writing that the proponent of the evidence claims it is including . . . two kinds of evidence . . . . It is well settled . . . that the testimony of a person who was present at the time a film was made that it accurately depicts what it purports to show is a legally sufficient foundation for its admission into evidence. In addition, . . . authentication of a photograph may be provided by the aid of expert testimony, as in the *Doggett* case, although there is no one qualified to authenticate it from personal observation. In *People v. Doggett* (1948) 83 Cal. App. 2d 405, 188 P.2d 792, the Court of Appeal upheld the admission of a photograph showing the defendants committing a crime. Because only the victim and the defendants, none of whom testified, were present when the crime took place and one of the defendants took the photograph, there was no one to testify that it accurately depicted what it purported to show. The People, however, produced evidence of when and where the picture was taken and that the defendants were the persons shown committing the crime. Furthermore, a photographic expert testified that the picture was not a composite and had not been faked. The court held this foundation sufficiently supported the photograph's admission as substantive evidence of the activity depicted. (*Id.* at p. 410, 188 P.2d 792.) [A] photograph may, in a proper case, be admitted into evidence not merely as illustrated testimony of a human witness but as probative evidence in itself of what it shows.[308]

306. These steps are derived from a logical dissection of the requirements of FED. R. EVID. 901.

307. 110 Cal. Rptr. 3d 362 (Ct. App. 2010).

308. *Id*. at 366 (some internal quotations and citations omitted).

This reasoning supports using surveillance video as the probe image for a face-matching computer system.

B. *Principles for Defendant Access to Face-Recognition Technology*

The standards for testing expert testimony on computerized face-recognition developed in Section V.A cannot be applied unless the defendant has access to the relevant details forming the basis for an expert's conclusions. When a computer generates photographs matching a probe image, the result is an out of court statement. When the match is introduced into evidence, it is offered to prove the truth the matching asserts—that the matching photograph matches the image of the perpetrator. Denying cross examination implicates the Confrontation Clause.

Trying to codify all the details of rules of procedure and rules of evidence is undesirable. Trial judges should be left a large degree of flexibility to use their own experienced judgment to manage the trials of particular cases. Accordingly, this Article does not suggest a statute or a model rule for cross examination of computerized face-recognition evidence. Rather, it offers some general propositions for judicial consideration.

- If the witness identification was substantially influenced by an image produced by a computerized face-recognition system, the defendant presumptively should be entitled to cross examine the witness about how she was influenced by the computer-generated image or images and to cross examine expert users of the computerized face-matching system.
- If the expert users and proponents of the computerized face-match are ignorant as to the content of the algorithms used to make matches and how machine learning was used to develop those algorithms, the defendant should be entitled to cross examine persons with such knowledge.

The caselaw on "*Wade* hearings," analyzed in Section IV.E.2, provides support for these two propositions.

C. *Questions to Ask*

The defendant in a criminal prosecution must keep her eye on the ball. The purpose of challenging computerized face-recognition is not to score points in public policy debates over use of the technology. The point is to exclude identification evidence or to cause the factfinder to doubt its reliability. So, if face-recognition technology has been used, not as the

primary identification evidence, but as a preliminary step in providing a foundation for subsequent human identification, the focus must remain on the reliability of the human identification. Typically, the defendant will challenge that reliability by arguing that the foundation for the identification was suggestive and therefore that it undermined the reliability of the identification. If the lineup or a photo array included only one black subject, then the witness said the perpetrator was black, that suggests that the only black subject was the perpetrator. Likewise, if the witness said the perpetrator was female and everybody in the lineup except one person is male, that is suggestive. The lineup and show up cases provide examples of how suggestions, such as these examples, can be established in closer cases.

Construction of templates or model questions for cross examining computerized face-recognition evidence should be informed by sets of model cross examination questions for fingerprint and DNA evidence publicly available on the Internet. Accordingly, the following list of questions include links to pertinent parts of suggested questions for fingerprint and DNA evidence.

1. Limitations of the Technology

Security Expert Clare Garvie makes three main criticisms of law enforcement agencies' use of the technology:

> 1. They use it ubiquitously and yet do not disclose when they are using it;
> 2. They use it improperly, resulting in false identifications; and
> 3. They obtain results that discriminate against darker skin probes and female probes.[309]

Her criticisms are worth scrutinizing. The second assertion, inaccurate face-recognition, may undercut the reliability of a match offered into evidence, or involve suggestivity of a human identification based on a computerized match.

Reliability depends on all the factors explained in Section II. An insufficiently diverse training database impairs the accuracy of the algorithms resulting from machine learning. Failure to use the best statistical inference methodologies likewise impairs the quality of the algorithms, regardless of how good the training database is. Poor quality probe images limit the reliability of efforts to match it with entries in an enrolled database. Images not included in an enrolled database cannot be selected as possible matches.

309. Garvie, *supra* note 49.

Suggestivity would occur if the investigators run a probe photo of any kind through a face-matching system, take only one of the matches based on the reliability score assigned to it by the system, and ask, "Did the perpetrator look like this?" The question for non-witness sources is "Do you know anyone who looks like this?" Presentation of the single image to a human witness is, indeed, suggestive. But this is not the equivalent of asking the face-recognition system, itself, "Do you know anyone who looks like this?" The human witness can accept or reject the computer-selected image.

If, on the other hand, the investigator shows only that photograph to a witness and tells the witness, "We ran the suspect through the world's best face-matching computer system, which has a 95% accuracy level. This is who that system says the perpetrator is. Do you agree?" That would surely be suggestive, and the human identification adds very little value to the identification made by the computer system. That does not mean, however, that the identification should be excluded from evidence. Rather, it highlights the importance of the defendant's right—reinforced by the Confrontation Clause—to probe the details of the computerized identification. If the computerized system is reliable, the suggested human identification is reliable; use of the computer system does not increase the probability of error.

Critics of the technology correctly observe that many probe images are of poor quality. The face-recognition system produces originals of enrolled images, usually of good quality. The witness looking at the array produced by the system has much higher-quality images to consider than if she looked at the probe image. This is not unusually suggestive, in itself. The witness is more likely to select one of the images rather than rejecting all of them, but that possibility is no different from a traditional lineup or photo array. The photo array provides a better basis for perception than the original glimpse at the perpetrator, which occurred in a time of stress, and usually was quite brief. That does not improve upon the original perception, however.

Picking one of the exemplars may be difficult when they are all generated by the face-recognition program. If it is working well, the possible matches all resemble each other. But that is the opposite of suggestiveness. It may be a basis for challenging the reliability of the identification, not on the grounds of suggestiveness, but on the grounds of randomness. How did the witness choose among quite similar faces?

Ms. Garvie reports use of a picture of the actor Woody Harrelson as the probe image for face-recognition as the basis for her "Garbage In, Garbage Out" title.[310] Even the Woody Harrelson example, which seems quite irregular, may have some justification. First of all, it's a reasonable

310. *Id.*

test of the system's accuracy. If Harrelson's photograph is used as a probe photo, the system should match it with a photo of Woody Harrelson. If it does not, that is a good reason to doubt the system's reliability.

That does not mean—hopefully—the law enforcement agency doing the match procures an arrest warrant for Woody Harrelson. Instead, the police are acting on a tip that describes the perpetrator as looking like Woody Harrelson. Using the face-recognition technique to identify people that look like Woody Harrelson is not unreasonable, *if* the results are used as the basis for further evaluation based on things like means, opportunity, and motive—the traditional indices of criminal involvement. The law enforcement agency should be given an opportunity to explain how it used the face-matching technology, why it used the probe image of Woody Harrelson, and what follow-up investigatory steps it took to identify the defendant. The identification of the defendant should not be rejected merely because face-recognition technology was used with a probe photo known not to be the perpetrator.

On the other side of the case, the defendant should know about the role face-recognition technologies played, and the defendant should be able to elicit the information about the Woody Harrelson probe, on the results obtained, and how those results were used for further investigation.

Similarly, there is nothing inherently outrageous about using an artist sketch as the probe image. The machine is being asked the same question as a human witness shown a traditional artist's sketches: "Does this look like the perpetrator? Do you know anyone who looks like this?"

2. Face-Recognition Trial Tactics

The proponent or opponent of computerized face-recognition evidence should be required to articulate methods and principles supporting a rational basis for a computerized face-matching expert's conclusions. As Section II.B explains, the validity of computer matching depends on the representativeness of the samples used to generate the matching parameters through machine learning. A factfinder should be able to evaluate the appropriateness of the database, and thus the parameters.[311]

Further, state-of-the-art machine learning algorithms for face-recognition use a variety of statistical measures, usually in combination with each other. Omitting some of these statistical steps can produce misleading results. The factfinder should be made aware of the state-of-the-art machine learning algorithms, the utility of each of the techniques,

311. *See* Transcript of Testimony at 69–70, United States v. Crawford, F2103-05 (D.C. Super. Ct. June 29, 2006), *available at* http://defensewiki.ibj.org/images/f/f9/Theisen_Budowle_Kittles_DNA_2006_06_29_Crawford.pdf [https://perma.cc/P57Q-38L2] (transcript of cross examination of DNA expert, concentrating on representativeness of database).

and how the party used these techniques in a particular product involved in matching a face in a specific case.

Then, the factfinder needs to know the types of errors that face-recognition programs can produce, and the available measures of the magnitude of likely errors. Any respectable computerized analysis uses statistical methods outputs of value that measures the statistical significance of its conclusion. Any face-match reported by such a program will be accompanied with a measure of probability that the reported match is valid.

At minimum, the factfinder needs to understand the difference between a false positive and a false negative. A false-positive may lead to a wrongful conviction; a false negative may lead to releasing a guilty defendant.

Reliability usually varies with the race, sex, age, and ethnicity of the subject, and it varies significantly with the quality of the images being compared. The factfinder should know the details of both images, in terms of the resolution,[312] focus of the image, lighting intensity and direction, and any artifacts that might result in distortion.

One defense counsel suggests focusing on the human decisions involved in use of automated face-recognition programs.[313]

3. Sample Questions

The foregoing discussion pertains to face-matching in general. Specific questions to be asked in a particular case must depend on how the face-matching program has been used. A one-to-one use, for example matching an on-scene snapshot of a potential suspect against surveillance imagery should evoke quite different questions from a one-to-many match. Indeed, one-to-many matches are less likely to be involved as evidence at trial, and more likely to be subject to challenge as the basis for reasonable suspicion or probable cause in earlier stages in the investigation and prosecution.

Effective counsel understands the limitations of face-recognition technology, such as the necessary resolution of digital images before it is reliable.[314] They also understand the limitations on machine learning,

---

312. Measured by pixels per square inch. King Catoy, *The Basics of Video Resolution*, VIDEO4CHANGE (Aug. 21, 2020), https://video4change.org/the-basics-of-video-resolution [https://perma.cc/Z6HY-PKQH].

313. *See* Jackson, *supra* note 147, at 14, 17.

314. *See* People v. Carrington, B265888, 2018 WL 671903 at *11 (Cal. Ct. App. Feb. 2, 2018) (evaluating testimony on face-recognition technology as applied to surveillance video to deny new trial; testimony suggests need for 60-120 pixels between the eyes of a subject for reliable face-recognition).

such as the number of training images available and their quality.[315]

In the interest of clarity, the following questions are somewhat open-ended, more suitable for depositions than for actual cross examination—for which skilled trial lawyers ask no question to which they do not already know the answer, and ask no question that cannot be answered by "yes," or "no."[316]

Questions for an eyewitness identifying the defendant in court:

- What did you use as the starting point for your identification of the defendant?
- You used an array of photographs, didn't you?
- You looked at individuals assembled in a live lineup, didn't you?
- You picked the defendant out of one or more individuals presented to you by the police outside of a police facility, didn't you?
- Who decided what photographs to include in the photo array? Who decided whom to include in the lineup?
- Who decided whom to include in the show up?

Questions for the designer of the lineup, show up, or photo array:

- How did you decide whom to include?
- What sources did you use for the images or life faces you included?
- What criteria did you use to pick someone for inclusion?

Questions for proponent of face-matching algorithms:

- Does your system use the Viola-Jones method for face detection?[317]
- Why or why not?
- Which of the following algorithms does your system use for feature extraction:

315. *See generally* Jackson, *supra* note 147.

316. *E.g.*, *Irving Younger's 10 Commandments of Cross Examination*, NEB. STATE BAR FOUND., https://www.nebarfnd.org/sites/default/files/2019-04/10commandments.pdf [https://perma.cc/DGP9-M9SF] (last visited Dec. 4, 2020).

317. *See* sources cited *supra* note 9.

  - AlexNet; Matthew Zeiler network; DeepFace; DeepID system; VGGFace; or FaceNew

- Why?
- Are you familiar with IBM's US Patent No. 9,990,537, "Facial feature location using symmetry line"?
- Describe its contribution to the state-of-the-art machine learning algorithms.
- Which of the following statistical techniques does your system use?
  - Principal Component Analysis; Linear Discriminant Analysis; Independent Component Analysis; Discrete Cosine Transforms; Gabor Filters; or Markov Models
- Why or why not?
- Which of the following approaches does your system use?
  - Microsoft; IBM; or Face ++
- Why?
- What other corresponding techniques does it use?
- How do you know that your training database was representative of the relevant population, in terms of demographic characteristics?
- Does your system make modifications to standardize face geometry?
- How many landmarks does your system use to define a face?
- What probe image did you use?
- Describe its quality, in terms of resolution, orientation, lighting, and focus.
- How many pixels represented the face, itself, in the probe image?
- Describe the contents of the enrolled database you used.
- Isn't it true that the perpetrator's image may not be in the enrolled database?

- What threshold does your system use to define a positive match?
- What threshold does your system use to define a negative match?
- Explain how your system's confidence values arise from statistical decision theory? Are they, for example, based on standard error calculations? If so, on what parameters?
- Did you compare the defendant's fingerprints with the FBI database to corroborate the face-match? What results did you obtain?

The questions that follow are adapted from a paper providing model cross examination questions for fingerprint examiners.[318]

- How many characteristics did the program use from the defendant's face?
- You did not determine how many characteristics from the possible matches matched characteristics from Mr. _____, did you?
- My client was identified solely based on a computerized face-match, wasn't he?
- He was identified based on photographs generated by a computerized face-matching program, wasn't he?
- The computer generates a list of candidates and ranks them according to how similar they are. Then you compare the defendant's to the candidates. Isn't that the way it works?
- But as soon as you find one that you think matches you stop. You do not look at the rest to see if they match better, do you?
- Here there were faces that the computer generated you never followed up on. So, you do not know if they are a better match?[319]
- You start from the premise that every face has different characteristics, don't you?

318. JENNIFER FRIEDMAN, MODEL CROSS EXAMINATION (FINGERPRINT EXAMINER) (Feb. 2017), https://www.wispd.org/attachments/article/242/Cross-Examination%20Fingerprint%20Examiner%20(Friedman%20REV%202-17).pdf [https://perma.cc/NRT2-L3FU].

319. *See id.* at 17–18.

- Do you know how many points or characteristics the average complete face representation has?
- [Ask the proponent of the system to cite his source for his statement.]
- So, the average full face has points or characteristics that could be compared, doesn't it?
- In this case, how many distinguishable points from the surveillance image were used?
- Sometimes you know information about the case, like why the police believe someone is a suspect, isn't that so?
- How many possible matches did the computer program output?
- How many of these did you show to the witness?
- Why did you exclude the others?
- Did you review the metadata for the candidate faces, such things as residence location, criminal history, and age?
- Did those match with what you know from interviewing witnesses and other evidence from your investigation?[320]

D. *Trade Secret Objections*

Rigorous cross examination about characteristics of commercial face-recognition products may encounter trade secret objections. The details of the algorithms used by the programs may well constitute trade secrets: information that has economic value by virtue of not being generally known and, with respect to which, the owner has taken reasonable precautions to keep it secret.[321]

Defense Attorney Kaitlin Jackson says that a challenger of computerized face-recognition will not be able to discover the algorithms used in the matching process, because they constitute trade secrets.[322] Whether these barriers are as high as Jackson says they are depends on the scope of privileges to resist a subpoena under Federal Rule of Criminal Procedure 17. Most trade secret cases involve civil discovery,

320. *See id.* at 8–10.

321. *See, e.g.*, HENRY H. PERRITT, JR., TRADE SECRETS FOR THE PRACTITIONER (6th ed. 2020) (defining and discussing trade secrets).

322. Jackson, *supra* note 147, at 21.

civil subpoenas under Federal Rule of Civil Procedure 45, or freedom of information act requests.[323]

Three solutions to this problem are available. The simplest is to exclude evidence if its validity cannot be tested through cross examination.[324] The second is to protect the cross examination from public disclosure. By closing the courtroom for that part of the trial and by issuing protective orders binding counsel, parties, and witnesses. Such measures frequently are taken to protect trade secrets in litigation.[325] Third, available only in some situations, is to recognize that trade secret protection is relinquished when one applies for a patent. The details of a patent are in the public domain. Even before a patent is granted or denied, patent applications are published.[326]

In the other contexts, the power to compel testimony constituting trade secrets depends on balancing the interest of the trade secret owner against opposing interests present in a particular legal context. In Freedom of Information Act cases, the interest opposing those of the trade secret owner is the general public's interest in knowing how their government functions.[327] In the civil litigation context, the interest of the requester relates to the requester's practical ability to make out a case or defense without the trade secret information.[328] The interest basically is the same whether trade secrets are requested in discovery or in court.

The interest of the trade secret owner is unambiguous: she will lose trade secret protection all together if the trade secret is disclosed to the public. In these several contexts, the interest of the trade secret owner can be protected by appropriate protective measures: prohibiting use or further disclosure by litigants and their counsel. Protective orders can impose these prohibitions during discovery. In the case of in-court trade secret disclosure, the testimony can be taken *in camera* or in a court room closed to the public, and any jurors can be prohibited from use or further disclosure. Reasonable measures to maintain secrecy is one of the

---

323. *See* PERRITT, *supra* note 321, §§ 4:9:5, 10:10.8 (freedom of information act requests); *see generally* Hannah Bloch-Wehba, *Access to Algorithms*, 88 FORDHAM L. REV. 1265, 1287 (arguing in favor of access to algorithms behind systems for breathalyzer and DNA evidence; emphasizing FOIA protections).

324. *See* discussion *infra* Section IV.D.1 (regarding Confrontation Clause).

325. *See* PERRITT, *supra* note 321, § 10:10.

326. 35 U.S.C. § 122(b)(1)(A) (providing for publication of applications 18 months after priority date).

327. *See* Chrysler Corp. v. Brown, 441 U.S. 281, 299 n.29 (1979) (describing tradeoff between public interest and effective functioning of government agencies).

328. *See Ex parte* Michelin N. Am., Inc., 161 So. 3d 164, 172–74, 182 (Ala. 2014) (granting writ of mandamus to protect trade secrets in products liability case; plaintiff failed to show necessity because of other ways to present case to jury; necessity means more than convenience and relevance).

elements of trade secret status, and such court-imposed limitations represent reasonable measures.

In the criminal context, the interest in the trade secret is the same, and can be protected by similar judicial protective measures.

The interests favoring disclosure are somewhat different, however. The scope of criminal discovery has long been limited,[329] and remains limited, even with recent reforms to expand discovery.[330] This suggests defendant interests in discovering trade secrets owned by third-party face-matching laboratories are weaker in the criminal context than in the civil context.[331] Confrontation Clause applicability also makes a difference in the interest analysis, leaning in favor of access. If the inability to access the trade secrets infringes the defendant's right to cross examine under the Confrontation Clause, his interests in obtaining access are correspondingly greater. Whether this is so in a particular case depends on the Confrontation Clause analysis of Section IV.D.1.

VI. LIMITING USE OF FACE-RECOGNITION BY LAW ENFORCEMENT

A. *Considerations*

Section IV.D.1 focused on the analysis of and strategies for dealing with hearsay and Confrontation Clause issues when face-recognition results are offered as evidence. This Section addresses a different question: whether limits should be imposed on the use of face-recognition programs. If policymakers decide that the law should place limits on police use of face-recognition, the more logical way to do it is to limit searches of enrolled databases. Imposing limits on capturing images of faces runs headlong into the lack of any reasonable expectation of privacy in one's face, and against the long-standing practice of taking mugshots. Limiting the creation of enrolled databases is also undesirable, because, at least in some circumstances, they are quite valuable in identifying

---

329. *See* Jenks Act, 18 U.S.C. § 3500(a)–(b) (denying defense access to witness statements until after witness has testified at trial).

330. *Compare* FED. R. CRIM. P. 16, *with* FED. R. CIV. P. 26(b). *See also* United States v. Al-Amin, No. 1:12–CR–50, 2013 WL 3865079 at *9 (E.D. Tenn. July 25, 2013) (observing that Rule 17(c) permits discovery subpoenas only when ordered by the court and only when the returns come to the court); United States v. Williams, CR419-089, 2020 WL 86814 at *2 (S.D. Ga. Jan 7, 2020); United States v. Durst, Criminal Action No. 15–091, 2015 WL 4879465 at *3, 4 (E.D. La. Aug. 14, 2015) (denying motion to quash Rule 17(c) subpoena and refusing to extend protective order to protect information not qualifying as trade secrets).

331. Rebecca Wexler, *Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System*, 70 STAN. L. REV. 1343, 1409–10 (2018) (arguing that trade secrets can be protected adequately in criminal proceedings by imposing conditions similarly to those in protective orders in civil cases); *id.* at 1403–09 (arguing that restricts on criminal discovery and subpoenas can adequately protect trade secrets without a separate privilege for trade secrets).

perpetrators of crimes, even if their use is limited. But even limiting searches of enrolled databases is undesirable because it forfeits a tool that makes identification more reliable and reduces false accusations. More specific requirements as to the characteristics of enrolled databases and searches of them is better policy than outright prohibitions.

One attractive model for limiting face-matching searches is the federal Stored Communications Act.[332] It is pertinent because it restricts database searches,[333] for example, of databases of emails,[334] and because the material to be searched is not protected by the Fourth Amendment, under *Smith*, because it is in the hands of third parties.[335] So protections of stored electronic communications, like possible protections against certain face-match searches, are purely statutory.

Of all the permutations identified in Section II.A and of all the law enforcement application described in Section III, the one most intrusive on reasonable expectations of privacy are many-unknown to many-known searches. While a member of the crowd does not have a reasonable expectation of privacy in his face, in the traditional sense, he may have a reasonable expectation of anonymity. That interest is eviscerated by effective crowds searching.

So, the starting point for statutory limitation might be to prohibit many unknowns to many knowns searches by law enforcement without some kind of court order.[336] Whether that court order should be a warrant depends on political judgment as to whether the well-developed probable cause standard is the appropriate one or whether a standard closer to articulable fact, as used in the Stored Communications Act, is preferable.[337]

The prohibition could permit exceptions upon some kind of factual showing. One possibility is to require the law enforcement applicant to articulate a reasonable suspicion that a fugitive or subject of an arrest

---

332. 18 U.S.C. §§ 2701–13.

333. 18 U.S.C. § 2701(a) (prohibiting unauthorized access to "wire or electronic communication" while it is in storage).

334. *E.g.*, O'Grady v. Superior Ct., 44 Cal. Rptr. 3d 72, 89–90 (Ct. App. 2006) (holding that Stored Communications Act covers email).

335. *See* Smith v. Maryland, 442 U.S. 735, 741 (1979); United States v. Miller, 425 U.S. 435, 443 (1976) (noting how police routinely access public domain or third-party services for facial recognition; they can enter a photo into an app which will search Instagram, Facebook and other social media to help generate leads).

336. On the other hand, court orders are not required for license plate searches. *See* Beaver, *supra* note 26 ("[L]icense plate readers . . . are basically a purely many unknown to many known check of license plates to detect possible crimes (stolen vehicles, expired plates, wanted subject owners, etc.). Where law enforcement would otherwise not know the person (car) was in the crowd, a reader allows law enforcement to detect it.").

337. 18 U.S.C. § 2703(d) (requiring "specific and articulable facts").

warrant is in the crowd or stream. Another possibility is to require the applicant to establish that traditional means of detection and identification have proven unsuccessful, as is the case with wiretap warrant applications.[338] The third possibility is to require the applicant to show that the purpose of the database search is to detect the presence of persons accused or convicted of serious crimes rather than petty crimes.[339]

Meeting any plausible standard for approval of a database search is easier when a one- unknown to many-known search is proposed. In such a case, the police have the image of an individual captured from the surveillance recording or created from witness descriptions. Then, the link between the subject and a crime is evident, and any reasonable standard prerequisite to a database search should be established.

Searching an enrolled database is not limited by the Fourth Amendment, because the subject whose probe image is being used has no reasonable expense expectation of privacy in the images in the database; those images belong to their subjects. Furthermore, the subject of the probe image has no property interest in the database. To be protected against governmental intrusion, the interest to be protected must be created by statute.

Analogies can be drawn to the caselaw on access to historic cell phone tracking data, which the Supreme Court determined was protected by the Fourth Amendment in *Carpenter v. United States*,[340] and Justice Sotomayor's concurrence in United States v. Jones.[341]

If many unknowns to many knowns become a routine tool of law enforcement purely out of efficiency, scans of every bus station, public building, and airport, would result in officers' just pulling people out of the crowd when something pops up. The result would be a significant diminution in historically availability anonymity. The best policy might be a prohibition on routine tracking all the time. Law enforcement could turn on the tracking and matching only when some reason exists to suspect a particular suspect is present or that a particular crime is being committed—wanted for one thing, catch or something else.[342]

---

338. 18 U.S.C. § 2518(1)(c) (requiring application for wiretap to state what other investigative procedures have been tried and failed or why they would be likely to fail).

339. *Cf.* 18 U.S.C. § 2516(1) (defining offenses for which wiretaps are available).

340. Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) (holding that venturing into public sphere does not negate expectation of privacy in movements revealed by historical cell site data); United States v. Elmore, 917 F.3d 1068, 1074 (9th Cir. 2019) (applying *Carpenter* and finding no probable cause).

341. United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring) (arguing that scope of Fourth Amendment should depend on breath of intrusion into subjects clothed with reasonable expectation of privacy).

342. Beaver, *supra* note 26. Beaver, *supra* note 47.

B. *Focusing on What Can Go Wrong*

The New York Times reported on a Detroit man who was arrested for a shoplifting incident he apparently had nothing to do with.[343] The article played up the fact that face-recognition software played a role in his identification. Face-recognition algorithms played a role, but he was not, as the headline and lead implied, arrested based solely on the computer-generated match. A loss prevention contractor for the store where the theft had occurred furnished surveillance video to the Detroit Police Department. The Police Department sent it to state police for use as a probe image for the state's face-recognition program. The face-recognition software reportedly generated a number of possible matches, including that of the arrestee.

The police generated a six-person photo array and showed it to the loss prevention contractor. She picked the arrestee's image from the array. It is not clear whether the array included only the possible matches generated by the computer program or whether it included images selected randomly or through other means. Nothing in the story suggests that the image corresponding to the computer-generated match of the arrestee received any special attention when the photo array was presented. The arrest thus was based on human identification, not on the computerized match.

If the police had not been able to use face-recognition software, either because it was unavailable to them or because the law prohibited its use, they could have done one of two things. They could have terminated their investigation for lack of evidence. The surveillance video still would have been available, but the police would not have had any ready means to link the image in the surveillance video to an actual person. Or, they could have used traditional human methods to match the surveillance video with mugshots and other types of photographs of people who might be possible suspects. Generating a photo array in that way, they could have showed it to the loss prevention contractor, and she might have selected someone who did not commit the crime.

Thus, taking face-matching technology out of the analysis, one can identify several specific sources of error. First, the quality of the surveillance image may have been so low that it lacked any utility as a starting point for identifying the perpetrator. Second, selection of images to include in the photo array may have been unprincipled, little more than random. Third, the human identification of one of the images in the array may have been unreliable.

---

343. Hill, *supra* note 93 (reporting on arrest of wrong man, based on identification of photo from "6-pack photo lineup" generated in part by face-recognition software supplied by DataWorks, NEC, and Rank One Computing).

A law prohibiting the use of computerized face-matching would not have eliminated any of these sources of error.

The law could address the sources of error by prohibiting the use of photo arrays altogether. It could prohibit the inclusion of a photograph in an array absent some level of suspicion, including full probable cause, to include that particular photograph. It could prohibit the use of surveillance camera images as the starting point for investigation and identification, at least if they fail to meet certain conditions of quality. A law or regulation specifically disfavoring computer-generated face-matching is appropriate only if empirical evidence shows that identification errors are more likely with the use of the technology than without it.

C. *Draft Statute*

Section 1 Definitions

Probe image: image of a person's face that the user of a face-recognition system seeks to a identify.

Enrolled database: A collection of images of faces of known individuals used in face-matching programs to see if any of the enrolled images match a probe image.

Training database: A collection of images of faces, expressed and organized for computer access, that present a wide variety of physical characteristics, enabling machine learning programs to develop algorithms for digital representation and comparison of faces.

One-to-one matching: Use of face-recognition software to determine if a known face-matches a pre-recorded phase.

One-to-many matching: a computerized face-match run in which the computer program seeks to match a single probe face against many facial images in an enrolled database.

Many-to-many matching: a face-matching computer run in which the user seeks to match several probe images against many facial images in an enrolled database.

Section 2 Prohibition on law enforcement use of face-recognition

No agency or officer of government, including persons or entities possessing law enforcement powers, shall use computerized face-matching technology except as provided in this act.

Section 3 Privileges

a. Any law enforcement officer may use one to one matching.

b. Any law enforcement officer may search an enrolled

database with a probe image obtained from video surveillance at a crime scene.

c. Any law enforcement officer or investigative agent may search an enrolled database with a probe image rendered by a sketch artist, or a sketch computer program based on a perpetrator description provided by witnesses.

d. Anyone may use a teaching database to develop face-matching software and hardware.

Section 4 Judicial authorization

a. A judge may authorize the use of computerized face-recognition systems beyond the privileges conferred in section 3, based on an application by law enforcement officers or investigative agents making the showing required by subsection (b)

b. the applicant for judicial order under this section must demonstrate by sworn testimony that:

i. Other traditional investigative means to identify a criminal perpetrator have been tried and failed;

ii. The applicant has reasonable grounds to believe that the source of the probe images to be used more likely than not contains the face of the perpetrator or of the subject of an outstanding arrest warrant or of a fugitive.

iii. Any face-match results of persons other than the identified subject must be destroyed after the face-match program is run.

Section 5 Report to Court

Whenever an order authorizing interception is entered pursuant to this chapter, the applicant must report to the judge who issued the order showing what progress has been made toward achievement of the authorized objective and the need for continued investigation. Such reports shall be made at such intervals as the judge may require.

Section 6 Discovery by Defendants

Upon a criminal discovery request, the state must disclose any use of face-recognition technology as part of the investigation leading up to the arrest of a defendant.

SURVEILLANCE CAPITALISM

William Hamilton[*]

In 2019, Harvard Business School Professor Shoshana Zuboff published *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*.[1]

What I hope to accomplish in this short presentation is to unpack some of the salient themes of this interesting, important book. I believe her book will lend context and urgency to this conference. Her book is a combination of excellent research, journalism, and scholarship. It is also a call, a plea, a supplication. Thus, the sub-title, *The Fight for a Human Future at the New Frontier of Power*, presages an unrelenting critical study of the deployment of a new economic power in the early 21st century.

However, a word of warning and a plea from me for indulgence. *Surveillance Capitalism* is a *tour de force* consisting of 525 pages of relatively small font text and over 100 pages of even smaller font footnotes. *Surveillance Capitalism* is not light reading. It is also hard reading: exciting and invigorating, but full of passion and indignation. I cannot hope to fairly present all her ideas, or even the depth of some of her ideas, in a short forty-five-minute presentation.

I will select those themes I deem most important for this conference, and I hope to inspire you to further plumb the depths of Zuboff's book.

Before diving into our exposition, a few references to a number of Western intellectual traditions will provide a helpful backdrop to the basic themes of *Surveillance Capitalism*. Shortly before the start of the workers' rebellions of 1848, a young Karl Marx drafted his *Economic and Philosophy Manuscripts*, articulating a theory of human alienation and expropriation in the industrial capitalist world that had been wrenched out of feudal landowning. Marx, of course, was no fan of feudal aristocracy, but he recognized something important in the rise of the factory and 19th century industrial capitalism. That salient fact was that capitalism stripped the worker of humanity is two ways. "Work of the hand" had become the "labor of bodies" toiling away during repetitive, monotonous, and often dangerous tasks. Second, the objects produced by the worker belonged to the factory owner. The craft worker makes a useful object, something of value. It has a ***use value***. I may trade it for other items, but initially it is the work of my hands that belongs to me. Industrial capitalism transformed work into factory labor, where products created by abstract and raw human labor power. The factory labor produced things that belonged to the owner by the means of production,

* Senior Legal Skills Professor, University of Florida Levin College of Law.

1. SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER (2019).

not the workers. The workers never owned the products of their labor. The products of their labor were immediately divorced from the workers and stood as objects of domination against the worker. Poverty ensued. Workers because fungible; all became the equivalent of laboring animals. The 19th century worker was thus paid a miserly salary inadequate to obtain the basic needs. Poverty was writ large in major European urban areas. As we shall see, these themes of expropriation, of theft, of taking, of ownership of the "means of production," are writ large in Zuboff's critique of the emerging power of surveillance capitalists in the 21st century.

These themes of industrial alienation and expropriation were articulated by many others in the 20th century, including Georg Lukács in his theory of commodity reification, *History and Class Consciousness*. Later, the intellectuals of the German Frankfort school articulated these themes, principally Max Horkheimer, Theodor Adorno, Erich Fromm, and Herbert Marcuse, who among other things, explored forces behind the fascist and communist totalitarian states. Marcuse, in particular, sought to explain the psychic distortions of 20th century capitalism in his influential book *One Dimensional Man*. An underlying theme of this tradition was the loss of human inwardness, autonomy, sense of self, and moral valuation arising from the new forms of social organization and production. This intellectual heritage was also carried forward by existentialist philosophers prior to and in the horrible aftermath of the World Wars.

A second 20th century intellectual tradition provides additional background. In the mid-twentieth century Vance Packard, a former advertising executive, published the *Hidden Persuaders*. The theme behind the work is that we are transformed into easily manipulated consumers by sophisticated and covert advertising forces informed by advances in psychological and sociological sciences. Packard continued this work in his second book, *The Naked Society*, where he criticized the use of increasingly available public information to manipulate essentially defenseless consumers.

Also, worth mentioning is a less well-known text by Jerry Mander, another escapee from the advertising world of the 1950s and 1960s. Mander's book is *Four Arguments for the Elimination of Television*. Mander himself has described the central theme of his book:

> [Television] organize[s] society in a certain way. [Television] give[s] power to a very small number of people to speak into the brains of everyone else in the system night after night after night with images that make people turn out in a certain kind of way. It affects the psychology of people who watch. It increases the passivity of people who watch. It changes family relationships. It changes understandings of

> nature. [Complex information that you] would get from reading … is flattened down to a very reduced form on television.[2]

Zuboff articulates similar concerns in the new and more frightening environment of the 21st century.

When I grew up in the 1950s and 1960s, we owned one small-screen TV for the family placed in small room. My brother and I were not permitted to watch TV on school days. Today, I have screens around my house, on my body, in my briefcase, in my office—and I have to fight with my students not to watch their screens during school days, but also in class. Our modern proliferation glass screens create a universe and dangers unthinkable at the beginning of the television.

Let's keep this in mind during our discussion today: for Zuboff, Facebook and Google and big tech are the tip of the spear, the petri dish, the incubator, the bellwether of the impact of the forces of surveillance capitalism unleashed upon us in what she calls a "coup from above." The constant, alienating, look so nicely articulated by Jean Paul Sartre, is now part of the fabric of our everyday life. We all know what it is like to try to perform even a routine task while under the critical gaze of the Other.

Today, our screens have become the glass walls of our lives, with the Big Other watching, extracting, and collecting the data of our lived lives.

The prior social critiques we have discussed were aimed at the 19th and 20th centuries. What is new about the 21st century that is so concerning to Zuboff?

Zuboff persuasively argues that something very new and very dangerous is loose in the land: that 21st twenty-first century surveillance capitalism is driven by a voracious demand for prediction, control, and guaranteed results. Surveillance capitalism is driven by the desire to collect massive amounts of data in order to predict, and ultimately control, (all) human behavior.

But what is so new about this claim? Advertising has always had an ugly underbelly that Vance Packard and Jerry Manders documented. Yes, advertising claims to promote consumer awareness and information. Yes, advertising claims to spur economic activity. Yes, advertising creates human wants at the expense of human needs. Yes, advertising ferments personal discontent, anxiety, and envy. Yes, advertising is driven by the purchase imperative and the goals of the seller. Yes, humans are vulnerable to the sophisticated and refined techniques of advertising typified in the hit TV series *Mad Men*. Again, what's new?

---

2. Wikipedia, *Four Arguments for the Elimination of Television*, https://en.wikipedia.org/wiki/Four_Arguments_for_the_Elimination_of_Television [https://perma.cc/Y357-47KE] (as of Nov. 21, 2020, 14:36 UTC).

What is new for Zuboff is the massively increased power and effectiveness of these influencers, the information about us they obtain and use, the methods of extracting this information, and the sophisticated algorithms deployed in the control project. It is as though advertisers from the 1950s woke up and found themselves in advertising heaven.

Let's take a moment to discuss this new power. Remember the subtitle of her book is *The Fight for a Human Future at the New Frontier of Powe**r***. Zuboff is not discussing power in the sense of government orders, violence, and physically compelled behavior. The power that Zuboff is concerned about is the power to nudge, push, cajole, edge, direct, and ultimately decide. This is her "new frontier of power." It is not rendition to a black site; it is not Mao Tse-tung's aphorism that "Political power grows out of the barrel of a gun."[3] It is power that is subtle, quiet, soft, enveloping, yet ultimately domineering and totalizing. It is power that hides behind such grand mission statements as: "*to give people the power to build community and bring the world closer together*" and "*to organize the world's information and make it universally accessible and useful*."

These perhaps originally noble, albeit naïve, mission statements, however, got perverted in the wake of the .com collapse. Suddenly, Silicon Valley had to make money for its investors. How? Suddenly, Silicon Valley discovered that it was sitting on mountains of gold. Salvation was in the trash, in the digital debris. Digital debris, digital breadcrumbs, digital exhaust, and digital waste provide big tech with the power to control our behavior while shrinking our sense of autonomy and moral foundations. It is the power to view the other as what is presented in the gold rush of extracted data artifacts. It is wonderfully (or horribly) morally neutral, driven only by the imperative to extract information from and about every aspect of our lived lives and to make perfect predictions and decisions. Whereas industrial capitalists of the 20th century found their fortunes in conquering nature (at the horrible price disrupted human relationships and in the form of climate change and species obliteration), the goal of the 21st century surveillance capitalist is to conquer human nature. We are its targets; we provide the abundant raw materials for the new means of production.

This new power of influencers is derived from our own creations. Let's consider primitive television advertising as an example. Do you remember the old commercial for StarKist tuna? It pictured an underwater tuna named Charlie doing artistic things like playing a violin, the piano, and singing classic melodies. Meanwhile, StarKist was fishing for tuna. But to Charlie's dismay, StarKist did not want to hook Charlie. StarKist rejected poor Charlie. StarKist wanted "tuna that tasted good,

3. *Mao Zedong: Quotes*, BRITANNICA, https://www.britannica.com/biography/Mao-Zedong/quotes [https://perma.cc/JNY6-RTDZ] (last visited Jan. 26, 2021).

not tuna with good taste." It was a pretty good commercial. I still remember it decades later. But I never purchased any StarKist tuna.

When did StarKist run these television commercials? Who was the audience? Somehow StarKist had to figure out how to maximize the impact of the commercial by reaching the audience that might purchase the StarKist product. Whatever the choice, the TV audience at any time was composed of viewers, like me, who either did not purchase food for the family or did not eat tuna. In short, the audience was always massively overbroad.

Let's move forward forty years. How many of you have had this experience? You are searching online for a product, say a cake dish, one evening. When you check your Facebook account the next day, low and behold, there is an advertisement for some brand of cake dishes. From an advertising point perspective, this is incredibly valuable. I get to market my product to a motivated consumer, and ***only to*** motivated consumers, dramatically cutting down the waste of traditional forms of television and print advertising. Today, I get advertisements all day long in my feeds, text messages, and searches about the things reflecting my online activity. As one Facebook executive stated, to paraphrase, we know so much about you we can direct you to the restaurant you want to go to when your plane lands in a new city. Think about it! This would be similar to a newspaper publisher being able to sell customized or particularized advertising to every subscriber. My neighbor would get the morning paper filled with advertisements about what my neighbor was doing yesterday, and I would get the same paper, but with different advertising about what I was doing yesterday. Every subscriber gets different so called "personalized" advertising. And we wonder why paper newspapers are struggling?

Here is the source of the original transgression by surveillance capitalism. Where did the surveillance capitalist get the information to target me with tailored advertisements? The information was stolen from me, excised, brazenly pilfered. It was extracted from my online behavior in the case of Facebook from likes, comments, posts, and the flood of digital gold rushing from our apps into analytic programs. Who gave Facebook the right to look at my searches, the feeds of my Friends, the comments of my friends, the locations of me and others like me **to determine how to manipulate and control me**?

How is this so-called "personalization" possible? A number of social preconditions are required. First, back forty years ago, there was little public information about me that could be easily harvested. Some, yes; massive amounts, no.

Today, as we all know, my personality is online. Facebook holds gigabytes of information about me (and 2.5 billion other accounts). Much of this information I have put on their webpage: pictures, posts, likes, comments, groups, friends, tags, etc. Additionally, Facebook obtains

voluminous information about me from other websites that I visit. This is called my Facebook offline activity. In the past few months, Facebook has provided a website that discloses some of the offline information sources supplying information to Facebook about our internet activity. I checked mine. The result: 124 of my favorite websites were sending information about me to Facebook that Facebook uses to continually refine its detailed profile of me. That profile is then used to sell advertisement placement on Facebook's pages, to nudge, push, incline, touch, poke, and prod me relentlessly. That is the secret strength of surveillance capitalists: they are relentless.

Here, we have one of Zuboff's major concerns and one of the sources of the indignation that flows through her book. My information is being turned against me! Data extraction is the compulsion and life blood of surveillance capitalism. Zuboff's critique recalls the young Marx's theory of alienation and theft of my labor by the 19th century capitalists. But now we have a new form of exploitation: the data about me. Zuboff focuses on what she calls data surplus, that information that is collected, extracted, and utilized to make predictions increasingly valid and accurate. Surplus value for Marx is what the capitalist steals from the factory workers by paying wages lower than the value of the factory production. For Zuboff, it is the excess of my digital activity; it is the content and metadata of my digital activity. The discovery of this surplus is for Zuboff the "game changing asset that turned Google into a fortune-telling giant."[4]

Facebook promotes itself as a way for me to keep in touch with my friends, neighbors and colleagues. I like this service. I use it. But what does Facebook do with my information? It turns my data against me by selling it to advertisers to nudge me in various directions; to peel away my privacy; and to investigate my soul. For example, Facebook says to an advertiser, "Do you want to sell books about 'law' and 'electronic discovery.'" We can identify a narrow group of likely purchasers and just advertise to them. Perhaps more alarmingly, as we all know, Facebook nudges and pushes not mere commercial products, but beliefs and political goals.

If you are a big spender, Facebook will even assign you specific advisors and experts to work closely with your campaign. Turning a moment to the political domain, Facebook was imbedded in the 2016 Trump election campaign. The Clinton campaign declined Facebook's offer. We all know who won the election out of nowhere. According to a recent report in *The Atlantic*, the Trump organization has a billion-dollar

4. ZUBOFF, *supra* note 1.

campaign planned for the coming election.[5] The Trump organization is rumored to have 1,000 data points about every U.S. voter.

Google is Zuboff's surveillance capitalist poster child. Google's search technology is beyond parallel. Page ranking is pure genius. Google also uses your searches to improve search. Google's algorithms can predict what I want to search even if my search is skewed and off mark. How does Google compute this? Easy. Just watch millions of others search to see their mistakes, selections, and corrections. This is Google using our searches to improve its search service. But what happened next was that Google had to make money. What is the solution: advertising! How can we create the best targeted advertising: use our customers search data! So suddenly, Google searches and research and development machines, composed of the best and brightest computer scientists, are perverted from the original goal of providing democratizing access to the web content. My searches have now turned against me, and the raw materials are collected, refined, crunched, and used to predict with incredible accuracy what I will do.

Zuboff's claim is that Google and other surveillance capitalists broke the critical link of reciprocity that help maintain 20th century social boundaries and bonds. Ford recognized that his workers had to buy his cars. Workers dwelling in a 19th century level of misery would not bring in revenues. So, workers were paid a wage that would allow them to purchase the basic commodities of 20th century existence.

Surveillance capitalists broke this social contract in numerous ways, but perhaps the most egregious is that Google did not merely use our searches to refine search and thereby produce a better product for us to use. The search activity of the Google user became the raw material of its predictions. Google applied sophisticated algorithms and machine learning to the search activity of millions of users to parse the torrents of digital information. Thus, began for Zuboff the conversion of the "raw material into the firm's highly profitable algorithmic products designed to predict the behavior of its users."[6] And it is not merely the actual search content that is mined, but all the artifacts surrounding the search: my diction, the length of the search, the particular search phrases, the time it takes me to compose the search, the time it takes me to enter the search, the hesitations in my search, the abandoned words and phrases, the frequency of the search, whether the search suggestions are followed and in what order, and so on. This is the secret sauce that reveals who we really are, but this is just the beginning of the story. Surveillance capitalism loves data processing, algorithms, and machine learning.

5. McKay Coppins, *The Billion-Dollar Disinformation Campaign to Reelect the President*, THE ATLANTIC (Feb. 10, 2020, 2:30 PM), https://www.theatlantic.com/magazine/archive/2020/03/the-2020-disinformation-war/605530/ [https://perma.cc/4VB2-T7A2].

6. ZUBOFF, *supra* note 1.

Surveillance capitalism is only possible because of the power of machines. My little iPhone can now perform a trillion operations a second. What amazing things engineers can do with a little silicon: dope it with a little boron and phosphorus, creating switches linked together that create billions of integrated circuits. We all know what machine learning can do: the algorithm learns from examples to identify similar content. This task sounds simple, but it takes immense computing power. Googles server farms crunch enough data to light cities.

In my area of professional specialization, litigation is now dominated by machine learning. We provide the software with examples of relevant documents, and then the software proceeds to rank the remaining documents in the collection as to how likely relevant. The software acts as a bloodhound tracking down relevant documents.

The bloodhound analogy is not far off. Law enforcement officials use facial recognition machine learning to track down and identify alleged criminals. Of course, the software is not perfect. A prediction is being made by the machine with a certain level of confidence. So, what are the risks in identifying criminals with only on a certain level of confidence? Law enforcement officials do perform good investigative police work, but law enforcement officials, like all humans, are very interested in justifying early decisions. I would not want to be a person falsely identified by a machine review of a database of facial images. These kinds of issues are discussed in *Weapons of Math Destruction, How Big Data Increases Inequality and Threatens Democracy*, by Cathy O'Neill.

But this is not Zuboff's point. Her point is that the surveillance capitalist imperative is to obtain more and more data. More data means better predictions. Better predictions means more revenues. The scary implication of her point is that, unchecked, surveillance capitalists will invade all aspects of our lives and appropriate one domain of lived experience after another.

Facebook, Google and certain others are the advance guard. I'm reminded of the scene from Kevin Costner's epic movie *Dances with Wolves*.[7] Costner plays a U.S. Army officer alone by force of circumstance on the U.S. Western frontier who forms a bond with a native American tribe. The tribal chief keeps asking the Army officer, "How many more whites will be coming?" The officer hesitates to answer. He knew the answer—and the looming result for native American people. As with the whites, more surveillance is coming and coming and coming, perhaps an unstoppable avalanche in the form of the "Internet of Things," smart devices, and sensors.

Let's take a simple, albeit hypothetical, example. Suppose I purchase a wonderful new vacuum cleaner that bounces around my house

7. DANCES WITH WOLVES (Orion Pictures 1990).

automatically vacuuming and sweeping the floors. This smart device is equipped with sensor technology that enables this wonderful time saving device go do its job. I can vacuum while I am at work! What a luxury. This smart device is WIFI connected, so that I can turn it on an off remotely and get software updates to improve performance. Sounds great. But what if the device is also mapping the interior of my home and creating a picture of my home's layout, furniture locations, rugs and carpet styles. What if it "knows" the kinds of debris on my floors: pet hairs, food crumbs, food crumb locations, lint, texture and fiber of my rugs, color of my rugs, etc. In short, my wonderful cleaning device is a mobile crime scene investigator that we may soon see in the TV series *Law and Order*.

In the movie *Elizabeth*, about the 16th century Protestant English Queen, the Catholic traitor Norfolk says he will be a martyr to the people once his head is chopped off.[8] The scene fades to darkness as Elizabeth's advisor Francis Walsingham steps back and whispers to Norfolk, "No, they will forget." They did, and Elizabeth prevailed, but our 21st century smart vacuum does not forget, ever. And what if all this information is being uploaded to our friendly vacuum cleaner manufacturer. And what if the manufacturer is selling this information?

The violation is twofold. Such a "smart" vacuum would likely be transmitting data without my knowledge and permission albeit covered by a legalist, extensive, and largely incomprehensible terms of a service contract or privacy statement. But more fundamentally, another domain of my life—my home—has been captured by the surveillance capitalist and is potentially being used to manipulate and control me. My home has become an open book; my sanctuary where I can be alone is lost. Yes, the information is valuable, but equally important is the fact that my home has now been what Zuboff calls "rendered," made available, disclosed, and exposed and in the process diminished. I believe Zuboff would say, "Stolen, expropriated, extracted."

For Zuboff, Google is at the front of the pack in misappropriating domains formerly thought beyond reach. Google has mapped my street and house for all to see in Street View. But this is my home and neighborhood, filled with the lives of my children, neighbors, block parties, accidents, divorces, and all the stuff of real existence. Google has made it a denuded treasure trove for gawkers, voyeurs, marketers, and realtors.

The infamous Google Glass is the perfect example of domain invasion by name and object. Google Glass was a product Google introduced some eight years ago. Google Glass was an inconspicuous miniature computer subtly attached to the frame of real or fake glasses. The camera "saw"

8. ELIZABETH (Gramercy Pictures 1998).

what I looked at. It recorded your personal interactions. Google Glass could ultimately detect lying by the facial tics, blinks, frowns, etc., of anyone I was speaking with. Simultaneously, all this information would be returned to Google. If I did not recognize someone, just look at the person and tap the glass and my database of pictures would find a match. I no longer needed a personal assistant at my shoulder reminding me of the names of people at parties. Everything I see became capable of being rendered. Google Glass is the constant accumulation of surplus data from the most personal aspects of our lives. Data that was never available is now rendered. How often do my students blink when I am lecturing in class? How often do my friends blink when I am at a cocktail party. This information was never before available to social scientists. Google Glass, a failed consumer experiment causing public outrage, is a metaphor. For the surveillance capitalist we are living in glass houses, glass offices, glass automobiles, glass streets, where everything can be expropriated for, of course, the common good.

So, for Zuboff, two things are happening. One previously unexplored domain of our lives after another is being invaded and catalogued by the technology grim reaper and the data that is being collected is being used for purposes driven by the behavioral modification goals of surveillance capitalism. We are all living in a giant Skinner box. For those in the audience not familiar with Skinner, he was a famous American psychologist who develop the theory of operant conditioning. All you need is the right pattern of stimulus and reward and any behavior can be created, modified, and adjusted. Problems at work? We have a behavior modification program for you and your co-worker. You will get along soon and be more productive. Our six-year-old neighbor, a wonderful little boy told us one day he was on a behavior modification program, a kind of token economy. For good behavior, he got a token in the jar he could redeem for things he wanted, e.g. candy. When we ask him how that was going, he replied he had a "negative balance." His parents did not have a very good program. But when he is on Facebook, his behavior will be more perfectly controlled and socialized?

Let's take another example. Truck accidents are a major highway concern. Truck accidents are caused in part by driver drowsiness. To combat driver fatigue, rules were implemented regarding the number of hours truck drivers can operate a truck. Sensors were placed in the vehicles to record operating hours. However, a new approach is being implemented: monitor the actual drivers' bodies with sensors. Cameras, hats, bands, and other devices with sensors are being attached to truck drivers to measure eye lid droop, head bobs and jerks, the various biometrics associated with fatigue. Brain waves are being measured and translated into predictions of alertness. All this is accomplished in the name of safety, an important social goal. But does anyone really think

that the information collected will not be used to decide who should and should not be employed?

A creepier example is the smart sleep mattress. It adjusts to movements, shapes, and body sizes to provide the most comfortable mattress shape. Of course, it can only work with a multitude of sensors. And the sensors need to be updated periodically with state-of-the-art software to make the smart mattress work even better for you. So that it can stay smart, it is WIFI connected. You can turn on the warming coils remotely when you are getting ready for bed. But what is being captured and transmitted to the mattress company are the hours you sleep and the regularity of your sleep. Add sound, and the mattress can tell if you have sleep apnea. And who knows what else it can sense about you in bed.

For the surveillance capitalist, nothing is sacred, and anything can be appropriated, stolen, rendered and co-opted. My house, my work, my office, my friends, my family, and my body, are all being digitized in the name of profit by private companies driven in the last analysis to maximize shareholder value. The distorted doctrine of shareholder value as the end-all-be-all of the corporation is horrible, but that is a different story.

Well, if all this is so terrible, how did we allow this to happen? First, Zuboff suggests, it snuck up on us. The Internet was originally perceived as a democratizing force. Technology was at the forefront of human advancement (and wealth). Our guard was down.

Second, there are benefits to the deployment of technology. We were seduced. The Internet is a vast repository of information; my colleagues and family are on social media sites; shopping is easier; and those ads are helpful at times. It was all too easy and comfortable for us to pay attention.

Next, Zuboff suggests that technology companies were less than forthright in their use of our information. They were and are secretive. To use another Hannah Arendt metaphor from the *Origins of Totalitarianism*, trying to expose the truth of surveillance capitalist operations is like peeling back the layers of an onion. So called privacy policies—what Zuboff calls "surveillance policies"—were crafted by lawyers using technical terminology and phraseology that few could understand and were presented as contracts of adhesion. If you want to be on Facebook, agree. If not, you are off. There is no negotiation, no choice, no compromise, no meeting of the minds. It is what Zuboff calls an un-contract.

Our ability to be shocked is being worn down. The constant creep of extraction of data surplus has a numbing effect. We have become habituated to its erosion so that hardly anything is shocking. Google Glass was too shocking eight years ago, but one wonders whether it would be today. Was it delivered just too early?

Importantly, Zuboff suggests that surveillance capitalists are willing to fight to the death to preserve their continued acquisition and use of data, to plumb new human lived experience, to continue the flow of gold. Data is the lifeblood of the surveillance capitalist. Think of it this way: your new, exciting app is designed to provide a minimal service, e.g. remind me to walk the dog and order special dog foods. Its real purpose is to collect data about you. The best apps cost little to develop and collect the most data, the most digital exhaust, the most breadcrumbs, and the most digital detritus. Acquisition is unrelenting imperative of the surveillance capitalist.

What are we to make of Zuboff's critique and where does it take us? First, the critique must be taken very seriously. We are in the fight of our lives. The future under surveillance capitalism is an addiction and a hollowed out human soul. It is Huxley's *Brave New World*, which of course was not brave or interesting, but an opiated world of control through drug addiction. Our future is a post-truth world of addiction to and participation in what Zuboff calls the Hive. Privacy, which Zuboff likens to ancient concept of sanctuary, is not merely threatened because some company may hold data about me. It is threatened on a more fundamental level because the goal of surveillance capitalism is to know everything about me to effectively manipulate and control me. Privacy does not merely mean the right to be left alone. It is the right not to have the digital artifacts of my life and body turned into alien objects that provide others a pathway to ***my*** soul and ***their*** riches.

Next, what is the path of resistance. I respectfully suggest that our traditional legal doctrines of contract, property, fiduciary duty, personal invasion, and copyright are inadequate to control surveillance capitalism.

The battle against surveillance capitalism in the United States is currently being structured in the language of full ***disclosures*** which is reminiscent of provisions of the Uniform Commercial Code from the 1950s. I submit that merely enhanced disclosure requirements will not blunt the continuing and unrelenting onslaught of data extraction and invasion. Indeed, the leading technology companies are being pushed to provide increasing disclosures, and technology companies are ironically posturing themselves as the protectors of privacy.

Google and Facebook constantly remind me to check my privacy settings and are involved in numerous public relations campaigns claiming privacy a personal responsibility. Is that really a fair battle, me against Facebook and Google? The knowledge asymmetry is dramatic. The surveillance capitalist has all the power, and I have none. And even if I were sufficiently motivated to study and keep abreast of what's happening to my data, can that be expect that of most users. Unfortunately, the workings of data networks, computer computational calculation, advanced analytics, machine learnings are beyond even

digitally literate consumers. The average consumer has no idea what a "cookie" is, what it looks like (text), and how browsers were originally defaulted to accept these text IDs placed on my machine by any website I visit.

Thus, we turn to regulations and laws as one of the principal methods to meeting the challenge of surveillance capitalism. Without restraining laws, the surveillance capitalist will relentlessly be collecting more and more raw surplus data. I suggest we need new laws dealing with this new challenge and a new federal agency charged with the task of enforcing the laws.

One bright light on the horizon is the European Uniform Domain-Name Dispute-Resolution Policy (UDRP), which is still in its infancy. Zuboff is hopeful that the UDRP is up to the task. However, the legions of attorneys of surveillance capitalism are on the march parsing every term to UDRP in an effort to weaken its reach.

I would suggest new U.S. "privacy" laws and regulations emerging in the United States take seriously the lessons of the General Data Protection Regulation (GDPR) regarding what I understand to be a few important provisions.

First, consumer data that is collected should only be used for the purpose intended and then immediately destroyed. A hotel does not need to keep records of my personal visit, e.g. how often I entered and exited my room using the smart key, once my visit is over. Should the hotel be permitted to keep information about me such as the age, make, brand, etc. of my vehicle gathered in video surveillance? Of course, as a general principle, data purging sounds reasonable, but in practice numerous problems emerge. The hotel may argue that keeping the data assists the company in providing better room service to know the average times guests are not in the room and the times most guests are in their rooms. Is this really a valid reason to amass customer data or a pretext for surveillance? And how is it enforced and monitored? How do we balance such claims against the user's rights?

Second, is consent. I suggest that enhanced disclosure and restricted consent is not the right direction for future laws. Consent requires knowledge, consent requires lack of coercion, and what I would call a lack of unfair leverage. Consent requires understanding the broad implications of the decision. We will soon see a shift by companies to persuade users to allow the exploitation of their data by such devices as price discounts, special privileges, and on a more coercive level, withdrawal of services.

The restrictions on the use of surplus data should be mandatory and the default provision. If consent is to be allowed it should be capable of being withdrawn. Additionally, consent must not be accompanied by any

inducements or encouragement, service refusals, or reduction in service quality.

A third suggestion is that new regulations rely heavily on: (1) private rights of actions, (2) expanded class action rights, and (3) significant liquidated fines for prevailing parties. Such regulations would create channels and incentives for the private bar to bring actions to enforce the new privacy regulations. Just as the earlier industrial state required unions and governmental laws and agencies to protect the social contract and fabric, so today we need the same.

Damages and remedies for the harms inflicted by surveillance capitalism is a perfect area for new legal scholarship. How can we define this new damage caused to individuals by surveillance capitalism? Private claims have been thwarted by a lack of causes of action and difficulty of defining and proving damages. Zuboff spends a significant amount of *Surveillance Capitalism* analyzing the harm data surveillance capitalism inflicts on adolescents and emerging adults in particular. Let us keep in mind what Zuboff has succinctly stated: the plaintiff is the force of the law.

A case in point is the current litigation under the Illinois Biometric Information Privacy Act.[9] Facebook recently agreed to a $550 million settlement and Google is facing similar litigation filed this past week. I will note that Facebook also agreed to a $5 billion fine with the Federal Trade Commission as part of the Cambridge Analytics settlement, but that was a data security issue more than a surplus data offense.

The question is whether these legal proceedings are really harbingers of things to come. The Illinois law only covers biometrics and has only been followed by Washington and Texas which do not provide for private rights of action. Meanwhile, California has enacted the California Consumer Privacy Act (CCPA), which protects biometric information and includes a private right of action.[10] Even if Zuboff's alarm is partially true, we are in the midst of a massive societal transformation that puts the future at risk and will require the highest level of attention, creativity, and collective action. The real question is what type of society do we wish to live in? Do we want a society that surprises children and emerging adults and causes them to engage in hiding activities to avoid the glasshouse environment?

Each semester in my e-discovery civil litigation class, we do a Facebook collection exercise so students will understand how to preserve, access, and evaluate potentially relevant information that may be in a Facebook account. I ask them to collect and inspect their own data and to let me know if anything caught their attention.

---

9. S.B. 2400, 95th Gen. Assemb. (Ill. 2008).
10. A.B. 375, 2017–2018 Session (Ca. 2018).

Here is just a small sample of their comments. Remember these are college graduates attending one of the nation's prestigious law schools.

> *I do not use facial recognition for Facebook, so it was surprising to see they were collecting facial data. Similarly, the folder labeled advertisers who uploaded a contact list with my info surprised me because most of these advertisers I have not shopped with or have involvement with.*
>
> *Some of the information that Facebook has of me either surprised me or made me do a "double take." For example, I was surprised they keep track of all the friends I've removed or friend requests that I've rejected.*
>
> *Facebook also keeps track of every search I've done. Even the deleted ones. I'm sure if everyone knew they could find every single search their partner has done; some awkward conversations would have to take place. For instance, "why were you looking her up?" I know I'm making a comedic instance out of this, but in reality, it is very weird that they track every single search and have it available for download.*
>
> *It also keeps track of every time I open the app, as well as all the IP addresses I've used to use Facebook. This is just weird because Facebook knows what you are up and where.*
>
> *I was able to go through all of my old messages starting from when I created my Facebook in 2008. I went down a Rabbit hole and then discovered my messages from my eighth-grade girlfriend.*
>
> *The second thing that surprised me was to see all the places I had checked in at and the fact that they had the geographical coordinates of the places that I checked in at.*
>
> *Also, I thought it was creepy how they save your search history.*
>
> *I was shocked by how long the list was and how many of the advertisers targeted ads were based on my browser shopping habits or random things that I had searched on Google when I was logged in to my Facebook account.*
>
> *Facebook has exact time stamps of when I liked and un-liked a friend. For years, they have kept this information. It is mind blowing to think of how much data they must have stored.*
>
> *I did not expect Facebook to collect my search history and locations. My instant reaction was to turn them off right*

> *away because I felt Facebook had become an invisible "spy" disguised as a friendly social media platform. Then, I started to wonder when on earth had I authorized Facebook to collect and store all my information.*

Is this the social environment we want where our best and brightest emerging adults are hiding and shocked by the practices of one of the world's most valuable companies?