WILMERHALE

WILMER CUTLER PICKERING HALE AND DORR LLP

The Long Term Enforcement Future for Privacy and AI

Kirk J. Nahra
WilmerHale
202-663-6128
Kirk.Nahra@wilmerhale.com
@kirkjnahrawork

Today's Discussion

- Some of the hot topics in privacy and AI today with an eye towards long term thinking about enforcement risks
- There are always changes with a new Administration
- There are always "counter-punches" from other aspects of government
- While it is of course critical to think about the environment today, I want to talk about the environment tomorrow

Today's Discussion

- We know there will be changes in the future
- These may be particularly significant – given how many changes are underway now
- A key point – just because its "ok" today does not mean it will be ok tomorrow

Today's Discussion

- A focus today on two areas:
- Long tail enforcement concerns
- "Consistent" enforcement concerns across administrations and time periods
- Some tips about thinking about these issues long term

Long Tail Considerations

Long Tail Considerations

- What do I mean?
- Areas where you may be “ok” today because of enforcement priorities - but there may still be issues with your decisions today in the (not too far off) future

False Claims Act – Cyber

- Relatively recent initiative of DOJ
- Also important whistleblower risks
- Has crossed Administrations at this point
- Meaningful look-back periods
- Can be tied to a specific incident or some other "prompt" – including internal understandings of CISO or others

Some Examples (False Claims Act)

- Illumina Inc. (2025) has agreed to pay $9.8 million to resolve allegations that it violated the False Claims Act when it sold to federal agencies certain genomic sequencing systems with cybersecurity vulnerabilities.
- The settlement resolves allegations that, between February 2016 and September 2023, Illumina sold government agencies genomic sequencing systems with software that had cybersecurity vulnerabilities, without having an adequate security program and sufficient quality systems to identify and address those vulnerabilities.

Some Examples (False Claims Act)

- Health Net Federal Services and its corporate parent Centene Corporation have agreed to pay $11,253,400 (2025) to resolve claims that HNFS falsely certified compliance with cybersecurity requirements in a contract with the DoD to administer the TRICARE health benefits program for servicemembers and their families.
- The settlement resolves allegations that, between 2015 and 2018, HNFS failed to meet certain cybersecurity controls and falsely certified compliance with them in annual reports to DHA that were required under its contract to administer TRICARE.

False Claims Act

- Repeated cases where cyber statements go back 8-10 years or more
- Can be triggered by a specific event or by many other developments
- Ongoing incentives for whistleblowers
- **Tip** – Pay close attention to internal concerns about security controls
- **Tip** - Don’t make certifications pro forma – do real ongoing evaluations

AI Enforcement Risks

- Particularly noticeable enforcement priority differences across Administrations
- Law is still developing – but developing rapidly
- Enforcement agencies aren't necessarily waiting for there to be "law"
- And a new enforcement agency in the future may look to creative ways to police behavior

AI Decisions - Former Regulators

- The trajectory of the Web 2.0 era was not inevitable — it was instead shaped by a broad range of policy choices.
- As the use of A.I. becomes more widespread, public officials have a responsibility to ensure this hard-learned history doesn't repeat itself.
- AI represents nothing special in the eyes of the law. "Although these tools are novel, they are not exempt from existing rules," . . . "and the FTC will vigorously enforce the laws we are charged with administering, even in this new market." (Lina Khan)

FTC - Consumer Protection Head (former)

- "We also have authority to prohibit and take action against "unfair" practices which are defined in our statute as practices that cause injury, that are not reasonably avoidable by consumers, and that don't have countervailing benefits to consumers or competition. If a company's data practices harm people, we're prepared to take action, even if those practices are accurately disclosed. In other words, we're not just looking at whether companies are telling the truth about how they're using people's data, we're thinking about whether companies are using people's data in a way that is likely to harm us."

AI Development

- Chair Khan - Sensitive personal data related to health, location or web browsing history should be “off limits” for training artificial intelligence models.
- The FTC is working to create “bright lines on the rules of development, use and management of AI inputs.” Khan said.
- “On the consumer protection side, that means making sure that some data — particularly peoples’ sensitive health data, geolocation data and browsing data — is simply off limits for model training.”
- Khan said that companies that want to use data they’ve already collected for AI training also must actively notify users of the change.

The FTC Now

- Very different approach
- New Chair - There will be “No more novel and legally dubious consumer protection cases.”
- "the pro-regulation side of the AI debate … is the wrong one," "a knee-jerk regulatory response will only squelch innovation, further entrench Big Tech incumbents, and ensure that AI innovators move to jurisdictions friendlier to them — but perhaps hostile to the United States."

AI Going Forward

- "Treating as categorically illegal a generative AI tool merely because of the possibility that someone might use it for fraud is inconsistent with our precedents and common sense. And it threatens to turn honest innovators into lawbreakers and risks strangling a potentially revolutionary technology in its cradle."

AI Moving Forward

- FTC Act "does not limit how someone who lawfully acquired those data might choose to analyze those data."

AI Future Thinking

- As with FTC efforts to create a law of privacy where there isn't one, a future FTC can look to create AI law
- We know how they have tried to do this in the past (both with data security standards and unfair privacy cases)
- Not only pursuing novel legal theories but also pushing boundaries on remedies

Disgorgement

- FTC has brought a series of cases where disgorgement of models has been a remedy
- A major impact on companies – clearly changes the risk management profile
- This is a real sanction - with real long tail implications

Disgorgement – Rite Aid

- Rite Aid allegedly failed to take reasonable measures to prevent harm to consumers from its use of facial recognition technology and violated a 2010 FTC order relating to data security and vendor management
- Factors supporting unfairness determination align with Biometric Information Policy Statement
- Rite Aid is prohibited from using facial recognition for five years; data and model deletion; consumer notice and redress; data retention
- settlement "offers a strong baseline for what an algorithmic fairness program should look like"

Disgorgement Issues

Rite Aid - In response to these alleged violations, the FTC is mandating that Rite Aid destroy certain algorithms. In its proposed settlement, the FTC orders Rite Aid to "delete or destroy all photos and videos of consumers used or collected in connection with the operation of a Facial Recognition or Analysis System…and any data, models, or algorithms derived in whole or in part therefrom…"

EVERALBUM

- The FTC finalized a settlement with the developer of a photo app that allegedly deceived consumers about its use of facial recognition technology and its retention of the photos and videos of users who deactivated their accounts.
- The FTC alleged that Everalbum, Inc. misled users of its Ever mobile app that it would not apply facial recognition technology to users' content unless they affirmatively chose to activate the feature. The company, however, automatically activated its face recognition feature—which could not be turned off—for all mobile app users except those who lived in three U.S. states and the European Union, according to the FTC's complaint.

EVERALBUM

- The FTC alleged that the company also failed to keep its promises to delete the photos and videos of Ever users who deactivated their accounts and instead retained them indefinitely.
- As part of the settlement with the FTC, Everalbum, Inc. must obtain consumers' express consent before using facial recognition technology on their photos and videos. The proposed order also requires the company to delete the photos and videos of Ever app users who deactivated their accounts **and the models and algorithms it developed by using the photos and videos uploaded by its users**.

Disgorgement

- Algorithmic disgorgement is the enforced deletion of algorithms developed using illegally collected data. As stated by FTC Commissioner Rebecca Kelly Slaughter, the rationale behind this remedy is that "when companies collect data illegally, they should not be able to profit from either the data or any algorithm developed using it."
- Some history – goes back to the FTC settlement with Cambridge Analytica in 2019.
- The Commission has since used algorithmic disgorgement in multiple subsequent settlements.

Disgorgement

- The FTC's December 2023 settlement with the Rite Aid Corporation was the first use of its Section 5 unfairness authority against an allegedly discriminatory use of AI.
- Led to an increased use of model deletion in future AI enforcement actions (with more expectations going forward).

Disgorgement - Guidance

- The FTC required the disgorgement of more than just the models that were allegedly improperly obtained.
- In the future - Any company developing models for machine learning or otherwise could face an FTC effort to obtain broad relief (perhaps beyond established claims or standards) and that FTC might seek disgorgement of assets that were not all improperly obtained so long as they are closely related to the issues underlying the investigation and were in some way obtained or used in violation of law of in another “unfair” way.

Disgorgement – Going Forward

- Be thoughtful about your decisions today (even if no one is currently watching)
- Be cognizant of any existing FTC agreements (even tangentially related) that can be used for future enforcement (with dollars)
- Be cognizant of how the FTC builds its "unfairness" jurisdiction
- Be thoughtful about permissions (both from consumers and commercial customers)

Criminal Issues

- DOJ Data Transfer Rules
- Privacy/HIPAA Criminal Cases
- Concerns today, long term concerns with events tomorrow
- Where potential criminal issues arise (e.g., a fraud claim) – be aware of how data issues can underlie the claims
- But hard to create “new” criminal law

De-Identification

- Evolving standards under existing and new law
- Growing technology concerns about re-identification risks
- Standards typically tied to current knowledge – but what happens “later” if there is re-identification?
- May not be a violation of de-id provisions – but is there some other kind of “problem”
- Be thoughtful about existing standards, real evaluations of risk, additional contract requirements, etc. (including DOJ rules where de-id data not exempt)

- Areas of Enforcement Consistency

Areas of consistency

- Children's Issues
- Bias (but not always the same kinds of bias)
- Health Care issues (but not always the same health care issues)
- Deception overall
- Cyber breaches (with long term review of practices)
- Data Brokers

Children's Issues

- Ongoing source of concern for state and federal regulators across administrations and red/blue states
- Real questions about appropriate ages
- Evolving areas of "actual" concern
- Future use of data about children when they are no longer children (think about permission status)

Bias

- Lots of attention to “bias” from former FTC
- Bias still being considered today – just different kinds of bias
- Privacy law is complicating the effort to “fix” bias in your models
- Think about and document how you are making decisions (particularly where consumer decisions/implications are significant)

Overall health data issues

- Lots of concern from lots of regulators about lots of health data issues
- Not likely to see FTC “making new law” in this area for now
- Continued state efforts – both law and enforcement
- Different areas of concerns (physician discrimination, transgender issues, differing views on Dobbs) – but ongoing activity

Deception Issues

- Consistent across administrations and red/blue states
- Public statements have a long life
- Whistleblower/FCA complicates things

Privacy issues

- Complexity of privacy law creates long tail issues
- Many laws address “size” issues – meaning that acceptable behavior for a small company is no longer appropriate after an acquisition
- Make sure that integrations happen effectively and that broader risk profiles are reviewed
- Similar issues as companies grow organically (without an acquisition)

Cyber Breaches

- Breaches will happen
- Having a good plan makes a lot of difference
- But when there is an incident there will be questions about what you have done – and what you knew and when you knew it.
- Continued issues through acquisitions
- Maybe not ten years of behavior but certainly five

Data Brokers

- Key focus of attention under state laws
- Key focus of attention in many state and federal investigations
- A challenging trail of data from multiple sources
- A potential disgorgement approach?
- Do you know your partners and vendors?

The State AG Counter-punch

- Need to keep states in mind today in response to changing federal priorities
- Certain areas (e.g., health care) we can expect aggressive state action
- In some areas not a red state/blue state issue
- Some red states very aggressive on data breaches and some kinds of privacy issues

Going Forward

- Continued deception cases
- Continued cyber breach cases
- Likely attention to children's data (although rules may change again)
- Much less activity on AI practices
- **Note - Keep an eye on the longer term**

How to Look Forward

- Cybersecurity remains enormously important (both because of enforcement and other problems)
- Take a longer view in advising clients (no enforcement now doesn't mean its legal)
- AI Perspective
- Be thoughtful about uses of sensitive data in any context

The Counter-punch - State AGs

- Likely continued focus on cyber incidents (both red and blue AGs)
- Likely increase in "privacy" enforcement from blue states
- Continued passage of new state laws (comprehensive laws, consumer health, Dobbs, other consumer issues, maybe AI)

Key Considerations

- Be thoughtful about relying on a no enforcement" approach from any administration guides legal advice and relevant decision making
- Be cognizant of uses of sensitive data
- Be conscious of bias and discrimination generally - to understand where there are potential gaps and how to think about them
- Think about your documentation over time, particularly on security policies
- Make sure you are fixing identified meaningful security problems

Questions?

Kirk J. Nahra
WilmerHale
202.663.6128
Kirk.Nahra@wilmerhale.com
@kirkjnahrawork