

The Washington Privacy Act

Chris Hydak, Microsoft

Saira Nayak, Privacy Salon

Hunter Ferguson, Stoel Rives

October 16, 2019

**Where We've Been, What We Saw,
Where We Might Be Going . . .**

TIMELINE

- Jan 18 – Senate Bill Introduced
- Jan 22 – Mar 5 – Senate Cmte Hrgs
- Mar 6 – Senate Bill Passed (46 -1)
- Mid-Late March – widespread prediction of passage . . . not so fast
- Mar 8 – House Takes Up Senate Bill
- Mar 22 – April 9 – House Cmte Hrgs & Amendments
- April 17 – Timed Out
- Legislative Session Resumes on Jan 13, 2020

THE BASICS OF THE SENATE BILL

- Covered “**legal entities**”
 - Conducting business in Washington or producing products or services targeted to Washingtonians; AND
 - Controls/Processes data of 100,000 consumers, OR
 - Derives >50% or revenue from sale and processes or controls personal data of 25,000 individuals
- Distinguished between **Controllers** and **Processors**
 - Processors required to assist controllers with meeting statutory obligations
- Employed typical definition of “**personal data**”
- Excluded **employment records**

THE BASICS OF THE SENATE BILL CNTD.

- **Consumer Rights**

- Right to Access
- Right to Correct
- Right to Deletion
- Right to Portability
- Right to Restrict Processing
- Right to Object to Processing
- Right against Exclusive Automated Decision Making

- **Controller Obligations**

- Privacy Notice
- Notify Third Parties re Changes to Personal Data
- Prompt Response (30 days)
- Profiling Disclosure
- Sale Disclosure
- Documented Risk Assessments

THE BASICS OF THE SENATE BILL CNTD.

- **Enforcement**
 - Washington AG
 - \$2500/\$7500 Penalty Structure
 - 30-day Cure Period
 - No Private Right of Action

THE BASICS OF THE SENATE BILL CNTD.

- **Facial Recognition**

- Controllers must employ meaningful human review when decisions produce legal or similar significant effects (e.g., financial, housing, insurance, employment, or health care services)

- Processors offering facial recognition services must provide documentation explaining capabilities and limitations

- Service agreements must prohibit use of facial recognition

technology for discriminatory activity

- Use of facial recognition technology in public spaces requires consent, which may be obtained through conspicuous notice (essentially opt-out)

- Providers of commercial facial recognition technology must make certain aspects of technology available for third party assessment and testing

- Gov't study

THE HOUSE BILL – WHAT CHANGED?

- Expanded scope of “**legal entities**” to include any entity doing business in Washington
 - Eventually revised to include add’l threshold criteria
- Recognized **consumer retention of ownership** interest in data
- Significant changes to **Facial Recognition** provisions
- **Private Right of Action**
 - Eventually withdrawn to include only AG Enforcement

THE HOUSE BILL – WHAT CHANGED?

- **Facial Recognition**

- Before using facial recognition technology, controllers and processor must verify absence of significant statistical variation on bases of protected immutable characteristics (*i.e.*, race, gender, national origin)
- Controllers may not use facial recognition for profiling
- Human review when decisions produce legal or significant effects required
- Use of facial recognition technology in public spaces requires specific, informed OPT-IN consent (mere notice/opt-out consent is insufficient)
- Notice required for automated decisions affecting the constitutional or legal rights, duties, or privileges of any Washington resident.

WHAT NEXT?

- Will we see a revived legislative initiative in Washington?
- Will a new bill be comprehensive or substantially narrowed in scope?
- Should we expect to see an effort to pursue seemingly controversial provisions that were not part of the initially successful Senate Bill?

WHAT NEXT?

- Do you think we will ever see a generally applicable privacy law in the US? Or will there always be some set of threshold criteria that must be met?
- What factors might open the door to including a private right of action?
- Should Facial Recognition Technology issues be addressed separately?
- Are the instrumental concerns about Facial Recognition Technology ameliorated through advances in the technology itself?
- How can the inherent concerns about Facial Recognition Technology be satisfactorily addressed? Do we just need “good” rules?

WHAT NEXT?

- What might the Washington Privacy Act mean for other state legislation? For ongoing federal legislative efforts?
- Are there legitimate concerns about interrupting free flowing interstate commerce? Are we seeing any market barriers create by state legislative efforts?
- Do national laws restricting data transfers teach us anything about what terms state laws should avoid?

Thank You

Chris Hydak, Microsoft
Saira Nayak, Privacy Salon
Hunter Ferguson, Stoel Rives
October 16, 2019