19.1041.02000

FISCAL NOTE

Requested by Legislative Council
02/05/2019

Amendment to: HB 1524

1 A. **State fiscal effect:** *Identify the state fiscal effect and the fiscal effect on agency appropriations compared to funding levels and appropriations anticipated under current law.*

	2017-2019 Biennium		2019-2021 Biennium		2021-2023 Biennium	
	General Fund	Other Funds	General Fund	Other Funds	General Fund	Other Funds
Revenues	$0	$0	$0	$0	$0	$0
Expenditures	$0	$0	$0	$0	$0	$0
Appropriations	$0	$0	$0	$0	$0	$0

1 B. **County, city, school district and township fiscal effect:** *Identify the fiscal effect on the appropriate political subdivision.*

	2017-2019 Biennium	2019-2021 Biennium	2021-2023 Biennium
Counties	$0	$0	$0
Cities	$0	$0	$0
School Districts	$0	$0	$0
Townships	$0	$0	$0

2 A. **Bill and fiscal impact summary:** *Provide a brief summary of the measure, including description of the provisions having fiscal impact (limited to 300 characters).*

The amended bill now calls for a study.

B. **Fiscal impact sections:** *Identify and provide a brief description of the sections of the measure which have fiscal impact. Include any assumptions and comments relevant to the analysis.*

No longer a fiscal impact to the Secretary of State

3. **State fiscal effect detail:** *For information shown under state fiscal effect in 1A, please:*

A. **Revenues:** *Explain the revenue amounts. Provide detail, when appropriate, for each revenue type and fund affected and any amounts included in the executive budget.*

N/A

B. **Expenditures:** *Explain the expenditure amounts. Provide detail, when appropriate, for each agency, line item, and fund affected and the number of FTE positions affected.*

N/A

C. **Appropriations:** *Explain the appropriation amounts. Provide detail, when appropriate, for each agency and fund affected. Explain the relationship between the amounts shown for expenditures and appropriations. Indicate whether the appropriation or a part of the appropriation is included in the executive budget or relates to a continuing appropriation.*

N/A

Name: Jim Silrum
Agency: Secretary of State
Telephone: 701-328-2900
Date Prepared: 02/05/2019

19.1041.01000

FISCAL NOTE

Requested by Legislative Council
01/14/2019

Bill/Resolution No.: HB 1524

1 A. **State fiscal effect:** *Identify the state fiscal effect and the fiscal effect on agency appropriations compared to funding levels and appropriations anticipated under current law.*

	2017-2019 Biennium		2019-2021 Biennium		2021-2023 Biennium	
	General Fund	Other Funds	General Fund	Other Funds	General Fund	Other Funds
Revenues	$0	$0	$0	$0	$0	$0
Expenditures	$0	$0	$80,000	$0	$0	$0
Appropriations	$0	$0	$80,000	$0	$0	$0

1 B. **County, city, school district and township fiscal effect:** *Identify the fiscal effect on the appropriate political subdivision.*

	2017-2019 Biennium	2019-2021 Biennium	2021-2023 Biennium
Counties	$0	$0	$0
Cities	$0	$0	$0
School Districts	$0	$0	$0
Townships	$0	$0	$0

2 A. **Bill and fiscal impact summary:** *Provide a brief summary of the measure, including description of the provisions having fiscal impact (limited to 300 characters).*

The bill creates a filing requirement with the Secretary of State for data brokers.

B. **Fiscal impact sections:** *Identify and provide a brief description of the sections of the measure which have fiscal impact. Include any assumptions and comments relevant to the analysis.*

In the bill, the only reference to the Secretary of State appears on page 2, line 16. It requires an annual registration with the Secretary of State on or before February first following a year in which the filer meets the definition of data broker. Because of several unknowns, the agency listed in 1A what it believes is the top end of a range of costs that may range down to only a few thousand dollars depending on the expectations of the legislature, which may require amendments to the bill to make it clear.

For example, if the only requirement expected of the agency is that it annually receives the data broker registration as a paper filing available to the public upon request that would require a minimal appropriation. However, if the data broker must also be registered as a “business” (page 1, line 13) entity (corporation, limited liability company, etc.), this will require more extensive programming. The programming would involve creating the online tools for registration, renewal of registration, amendments, cancellations, the issuance of certifications, automated jobs for renewal notices or going out of “good standing” status if the business fails to file its annual report, receipt of fee payments, public search of these registrations, what information is and is not available to the public, etc. When these and other unknowns are identified, the agency will be better able to estimate the cost.

3. **State fiscal effect detail:** *For information shown under state fiscal effect in 1A, please:*

A. **Revenues:** *Explain the revenue amounts. Provide detail, when appropriate, for each revenue type and fund affected and any amounts included in the executive budget.*

It is unknown as to the what the sponsors have estimated to be the number of registrations that would result. Based on whether ten file, it would result in revenue of $1,000. The bill do not indicate if the registration fee would be deposited in the general fund or the agency's general services fund.

B. **Expenditures:** *Explain the expenditure amounts. Provide detail, when appropriate, for each agency, line item, and fund affected and the number of FTE positions affected.*

The extent of the expenditures is unknown because the scope of the expectations is not identified.

C. **Appropriations:** *Explain the appropriation amounts. Provide detail, when appropriate, for each agency and fund affected. Explain the relationship between the amounts shown for expenditures and appropriations. Indicate whether the appropriation or a part of the appropriation is included in the executive budget or relates to a continuing appropriation.*

The needed appropriation will depend on the expectations of the legislature.

Name: Al Jaeger

Agency: Secretary of State

Telephone: 701-328-2900

Date Prepared: 01/18/2019

2019 HOUSE INDUSTRY, BUSINESS AND LABOR

HB 1524

2019 HOUSE STANDING COMMITTEE MINUTES

Industry, Business and Labor Committee
Peace Garden Room, State Capitol

HB 1524
1/21/2019
31135

☐ Subcommittee
☐ Conference Committee

Committee Clerk: Ellen LeTang

Explanation or reason for introduction of bill/resolution:

Regulation of data brokers.

Minutes: Attachment 1, 2 , 3

Chairman Keiser: Opens the hearing on HB 1524.

Rep Mock~District 18: Attachment 1 & 2. The second attachment is an amendment that is a hog house.

9:35

Rep P Anderson: In all you research, is the federal government going to do anything?

Rep Mock: There is a big question mark. I would like to see one set of policies, because we don't know what congress is going to do. I would like to see ND be a leader with reasonable definitions in working with industry, consumer's advocates.

Rep P Anderson: Is it a concern that it will be pushed under & then it will be worse?

Rep Mock: It's so new that we haven't seen any effects yet. It's too early to tell.

Rep Kasper: I have contacted the technology industry & they are willing to engage. It will be interesting what we will find out.

Rep Mock: I agree.

Chairman Keiser: Page 2, line 21, we have to opt in before they share. We don't think that we want data brokerage telling us that we can opt in or opt out. Just a thought.

Rep Mock: This section is related to the registration. A data broker that registers through the state of ND, this is one thing that needed to be disclose that for the opt out in their

registration. It's more of a disclosure on what the processes of the data brokerage by & not a requirement or expectation that they do.

Chairman Keiser: Anyone else here to testify in support, opposition, neutral position?

17:10

Jim Silrum~Deputy Secretary of State: With a quick google search, the registering of these, there are 3,5000 to 4,000 legit data brokers. Free lancers are playing a bigger role. Getting our arms wrapped around the concept of reaching out to all of those that they have a registration requirement, we would ask the committee to consider that as part of it.

Chairman Keiser: Good point Jim.

Jerry Ketterling~Native of ND: I'm excited to see some legislation coming forward that is offering some data privacy for the citizens of ND. The definition of a data broker is the one concern on this bill. By definition, does that include the state of ND? We are in the business of collecting data & it has been used in the past years for educational funding & selling of information for return on investments. It needs to be looked at of what the ramifications are to the state. As well as, what overall is missing, I don't see data privacy being address.

I see some value towards the bill, but I think there needs some rewrite with emphasis on data privacy, first & foremost. We could take the position of providing data privacy to our citizenry in the form of opt out or opt in. Right now, by definition, it's opt out. It would be nice to see if we could move the state towards an opt in. What I'm looking at is it's a great start & we need to have something.

However, I'm concerned about the punitive damages that are not defined here. My experience in my world, nobody does anything until there is punitive damages behind it. I don't want legislation that takes a stick after innovation. In data brokerage, all the free services & cool things we enjoy in our house. How many are willing to give up their toys?

From the state's perspective, what I want to see in a bill like this, is punitive damages defined, right to notification of date breach immediately, within 45 days & a definition of what a data brokerage is.

21:05

Rep Kasper: In HB 1485, it's all in there.

Chairman Keiser: Closes the hearing.

Alexi Madon~Director-State Government Affairs-Midwest: Attachment 3. Submitted testimony, but did not attend.

2019 HOUSE STANDING COMMITTEE MINUTES

Industry, Business and Labor Committee
Peace Garden Room, State Capitol

HB 1524
2/4/2019
32063

☐ Subcommittee
☐ Conference Committee

Committee Clerk: Ellen LeTang

Explanation or reason for introduction of bill/resolution:

Regulation of data brokers.

Minutes:

Chairman Keiser: Reopens the hearing on HB 1524.

Chairman Keiser: What are your wishes? The hog house simply converts it to a study.

Rep D Ruby: Move the amendment 19.1041.01001. It simply converts this to a study.

Vice Chairman Lefor: Second.

Chairman Keiser: Before we jump into the fire, we need to do some studies.

Voice vote ~ motion carried.

Chairman Keiser: What are you wishes?

Rep D Ruby: Do Pass as Amended.

Rep Schauer: Second.

Chairman Keiser: Further questions?

Roll call was taken on HB 1524 for a Do Pass as Amended with 14 yes, 0 no, 0 absent & Rep C Johnson is the carrier.

DA 2/9/19

19.1041.01001
Title.02000

Prepared by the Legislative Council staff for
Representative Mock
January 21, 2019

PROPOSED AMENDMENTS TO HOUSE BILL NO. 1524

Page 1, line 1, after "A BILL" replace the remainder of the bill with "for an Act to provide for a legislative management study of privacy practices in the data broker industry.

BE IT ENACTED BY THE LEGISLATIVE ASSEMBLY OF NORTH DAKOTA:

SECTION 1. LEGISLATIVE MANAGEMENT STUDY - DATA BROKER INDUSTRY. During the 2019-20 interim, the legislative management shall consider studying privacy practices in the data broker industry to determine whether adequate safety measures exist to prevent fraud and protect the identifying information of consumers. The study must include consultation with the department of commerce and the attorney general, and an evaluation of the nature and sources of the consumer information the data brokers collect, how data brokers use, maintain, and disseminate the information, and the extent to which the data brokers allow consumers to access and correct their information or to opt out of having their personal information sold. The legislative management shall report its findings and recommendations, together with any legislation required to implement the recommendations, to the sixty-seventh legislative assembly."

Renumber accordingly

Date: Feb 4, 2019

Roll Call Vote #: 1

2019 HOUSE STANDING COMMITTEE
ROLL CALL VOTES

BILL/RESOLUTION NO. 1524

House Industry, Business and Labor **Committee**

☐ **Subcommittee**

Amendment LC# or Description: 19.1041.01001

Recommendation

☒ Adopt Amendment
☐ Do Pass ☐ Do Not Pass ☐ Without Committee Recommendation
☐ As Amended ☐ Rerefer to Appropriations
☐ Place on Consent Calendar

Other Actions ☐ Reconsider ☐ _____

Motion Made by Rep Ruby **Seconded By** Rep Lefor

Representatives	Yes	No	Representatives	Yes	No
Chairman Keiser			Rep O'Brien		
Vice Chairman Lefor			Rep Richter		
Rep Bosch			Rep Ruby		
Rep C Johnson			Rep Schauer		
Rep Kasper			Rep Adams		
Rep Laning			Rep P Anderson		
Rep Louser			Rep M Nelson		

Total (Yes) _____ No _____

Absent _____

Floor Assignment voice vote - motion carried

Date: Feb 4, 2019

Roll Call Vote #: 2

2019 HOUSE STANDING COMMITTEE
ROLL CALL VOTES

BILL/RESOLUTION NO. 1524

House Industry, Business and Labor **Committee**

☐ **Subcommittee**

Amendment LC# or Description:

Recommendation

☐ Adopt Amendment
☒ Do Pass ☐ Do Not Pass ☐ Without Committee Recommendation
☒ As Amended ☐ Rerefer to Appropriations
☐ Place on Consent Calendar

Other Actions ☐ Reconsider ☐

Motion Made by Rep Ruby **Seconded By** Rep Schauer

Representatives	Yes	No	Representatives	Yes	No
Chairman Keiser	X		Rep O'Brien	X	
Vice Chairman Lefor	X		Rep Richter	X	
Rep Bosch	X		Rep Ruby	X	
Rep C Johnson	X		Rep Schauer	X	
Rep Kasper	X		Rep Adams	X	
Rep Laning	X		Rep P Anderson	X	
Rep Louser	X		Rep M Nelson	X	

Total (Yes) 14 No 0

Absent 0

Floor Assignment Rep Johnson

REPORT OF STANDING COMMITTEE

HB 1524: Industry, Business and Labor Committee (Rep. Keiser, Chairman) recommends **AMENDMENTS AS FOLLOWS** and when so amended, recommends **DO PASS** (14 YEAS, 0 NAYS, 0 ABSENT AND NOT VOTING). HB 1524 was placed on the Sixth order on the calendar.

Page 1, line 1, after "A BILL" replace the remainder of the bill with "for an Act to provide for a legislative management study of privacy practices in the data broker industry.

BE IT ENACTED BY THE LEGISLATIVE ASSEMBLY OF NORTH DAKOTA:

SECTION 1. LEGISLATIVE MANAGEMENT STUDY - DATA BROKER INDUSTRY. During the 2019-20 interim, the legislative management shall consider studying privacy practices in the data broker industry to determine whether adequate safety measures exist to prevent fraud and protect the identifying information of consumers. The study must include consultation with the department of commerce and the attorney general, and an evaluation of the nature and sources of the consumer information the data brokers collect, how data brokers use, maintain, and disseminate the information, and the extent to which the data brokers allow consumers to access and correct their information or to opt out of having their personal information sold. The legislative management shall report its findings and recommendations, together with any legislation required to implement the recommendations, to the sixty-seventh legislative assembly."

Renumber accordingly

2019 SENATE INDUSTRY, BUSINESS AND LABOR

HB 1524

2019 SENATE STANDING COMMITTEE MINUTES

Industry, Business and Labor Committee
Roosevelt Park Room, State Capitol

HB 1524
2/27/2019
Job #32917

☐ Subcommittee
☐ Conference Committee

Committee Clerk: Amy Crane

Explanation or reason for introduction of bill/resolution:

A BILL for an Act to provide for a legislative management study of privacy practices in the data broker industry.

Minutes: Att. #1-2

Chairman Klein: Opened the hearing on HB 1524. All members were present.

Representative Beadle, District 27: see attachment #1 for testimony in support of the bill.

Senator Burckhard: There's a fiscal note with a lot of zeroes what's up with that?
Representative Beadle: The original bill that had all of the licensing and everything else in there did have a fiscal note on it, because we were adding new licensing, framework, everything else, after the amendment to put it down to a study, the fiscal note got zeroed out.

Chairman Klein: I'm guessing you're aware of Representative Kasper's bill. Is that similar?
Representative Beadle: I think they are fairly similar, originally they were two different cogs that were working in a similar direction but were touching on slightly different areas. This one was more broad in terms of what the state needs to do for regulatory framework and everything else. So they were basically related but not directly. We could certainly bridge the gap on those and make whichever the viable one the vehicle going forward. We just want the state involved so we can do what we need to to protect our constituents.

Chairman Klein: Just so you know Representative Kasper wants to put his back to the way it was.
Representative Beadle: I'm sure, and this one could be put back to the way it was as well.

Chairman Klein: I think we understand this privacy issue is big stuff and we need something to continue so that we have this at least during the interim to work on.
Representative Beadle: Nothing on this one specifically goes into if someone is spoofing accounts or creating fake accounts. I think we have other fraud statutes that may be able to deal with that but I know the committee may have some concerns about that portion of cyber security and data protection this wouldn't address that but I just wanted to make sure the

committee knew that. this is touching the whole social media world but not specifically that issue.

Senator Piepkorn: When I go to messenger on my phone it tells me we've transferred all of your data over, and it asks me to accept so many terms but do you know what I mean?
Representative Beadle: I'm aware of what you mean. The issue specifically with the switch to messenger is that Facebook was previously operating two separate electronic messaging systems, one that was fully integrated into the Facebook app and one that was a standalone messenger feature. When they rolled out and fully leaned into the messenger feature they migrate all of their in-house stuff on the Facebook platform to the stand alone one, so that is why you are getting those notifications. Because while it's under the Facebook umbrella it can stand alone as its own entity. From an advertising perspective you can send ads through the messenger app.

Senator Piepkorn: So I accepted the next thing and it says messenger text and video chat for free needs access to identity, contacts, location, SMS, phone, photos, camera, WIFI, device id.
Chairman Klein: Is that what we're studying?
Representative Beadle: Essentially yes, that's all data. That is all your consumer data. Because Facebook and entities like that are collecting your data and then offering that up to both on the aggregate where it's not user-identified but then also through their advertising platform so that an advertising company can go in there and target certain customers. We can micro target people based on that level of consumer data. That's your information that gets shared. We're saying that if you're an entity that is collecting and selling this data, we need to make sure that we have some level of regulation or oversight to ensure that you're treating that data with the care it deserves. Originally this bill would have put some North Dakota protections on it. Now it's just studying it to see what's happening out there and we pivot accordingly.

Senator Piepkorn: Just as a matter of record, I haven't accepted all that.
Representative Beadle: If you have the app on your phone then they have your data.

Senator Roers: Could you expand just a little bit. So there has been issues with Amazon and Alexa listening to your conversations 24/7. Google, Twitter, and LinkedIn is where that data is accumulating?
Representative Beadle: Google is collecting it if you have the Google home system. Amazon is collecting it if its Alexa. All of those would qualify under consumer data that we're looking at in terms of where your data is going, who is collecting it, and what they are doing with it and making sure you are protected. While I use Facebook, Twitter, LinkedIn, etc. as examples, I only use those because they are very wildly known but there are hundreds that would operate in this sphere collecting and disseminating data.

Senator Burckhard: So Marriot was breached a while back and 500,00 customers, so basically the mea culpa was just oops our bad?
Representative Beadle: That has basically been the case so far. There have been occasional slaps on the wrist, a lot of that is federally regulated. What was it the Experian hack that had 1/3 of the country's data. There is a lot of consumer data that is out there and people know how to make money off of it. Using that information to better develop that and

create new technologies, that's good uses of data. Or if it's through back channels and the dark web. This is just making sure that we have a study vehicle so that we can see what's going on and properly respond.

Senator Kreun: What are we gonna gain from this? What will be the result of the outcomes of the study?
Representative Beadle: We have to study that and find out.
Chairman Klein: But I believe there are stakeholders now that are observing this and seeing it pop up in other states and working together.

Representative Beadle: Once, California passes something that involves the IT world and enforces it, every single company responds. As we see the full rollout of the legislation they passed last year, as well as how the conversation goes federally, we might be in a situation where we don't have to do anything in North Dakota but it's important for us to be abreast of what's going on.

Levi Andrist, on behalf of Gabby Reed, Manager, RELX and LexisNexis: See attachment #2 for testimony in opposition to the bill.

Chairman Klein: What you're suggesting is 1524 could go away and 1485 could stand in, would be a better vehicle?
Levi: Yes, and if you look at the language, 1485 is more broadly worded so you'd be studying more under that bill.

Senator Roers: Didn't they both pass the house?
Levi: As studies yes.

Senator Roers: So would they come together at a joint committee?
Chairman Klein: We would make that decision. So what we're going to do is hold off until we hear 1485 and then we will move on of those forward. I think there is some conversation that they want something more than a study passed. So we may need a study in addition to the comprehensive bill that we will pass?

Lacee Anderson, Match/MidCo: testified in opposition. I echo what Levi said, we're in the same position on 1485 and feel that would be a better study. But we still highly encourage a study in this regard there is just not enough information out there.

Chairman Klein: So one way or another we need something to come out of this as a study?
Lacee: Yes.

Chairman Klein: Closed the hearing on HB 1524.

2019 SENATE STANDING COMMITTEE MINUTES

Industry, Business and Labor Committee
Roosevelt Park Room, State Capitol

HB 1524
3/19/2019
Job #33921

☐ Subcommittee
☐ Conference Committee

Committee Clerk: Amy Crane

Explanation or reason for introduction of bill/resolution:

A BILL for an Act to provide for a legislative management study of privacy practices in the data broker industry.

Minutes: None.

Chairman Klein: Opened the committee work session on HB 1524.

Chairman Klein: This was the bill that piggy backed on 1485. We can reconsider our actions on that or we could pass this one.

Vice Chairman Vedaa: 1485 is a shall study and 1524 is a shall consider.

Senator Roers: Moved a Do Not pass.

Senator Burckhard: Seconded.

A Roll Call Vote Was Taken: 6 yeas, 0 nays, 0 absent.

Motion Carried.

Chairman Klein will carry the bill.

Date: 3/19
Roll Call Vote #: 1

2019 SENATE STANDING COMMITTEE
ROLL CALL VOTES
BILL/RESOLUTION NO. 1524

Senate Industry, Business and Labor Committee

☐ Subcommittee

Amendment LC# or Description: _____

Recommendation: ☐ Adopt Amendment
☐ Do Pass ☒ Do Not Pass ☐ Without Committee Recommendation
☐ As Amended ☐ Rerefer to Appropriations
☐ Place on Consent Calendar

Other Actions: ☐ Reconsider ☐ _____

Motion Made By Roers Seconded By Burckhard

Senators	Yes	No	Senators	Yes	No
Chairman Klein	X		Senator Piepkorn	X	
Vice Chairman Vedaa	X				
Senator Burckhard	X				
Senator Kreun	X				
Senator Roers	X				

Total (Yes) 6 No 0

Absent 0

Floor Assignment Klein

If the vote is on an amendment, briefly indicate intent:

REPORT OF STANDING COMMITTEE

HB 1524, as engrossed: Industry, Business and Labor Committee (Sen. Klein, Chairman) recommends **DO NOT PASS** (6 YEAS, 0 NAYS, 0 ABSENT AND NOT VOTING). Engrossed HB 1524 was placed on the Fourteenth order on the calendar.

2019 TESTIMONY

HB 1524

NORTH DAKOTA HOUSE OF REPRESENTATIVES

STATE CAPITOL
600 EAST BOULEVARD
BISMARCK, ND 58505-0360

Representative Corey Mock
District 18
P.O. Box 12542
Grand Forks, ND 58208-2542
C: 701-732-0085
crmock@nd.gov

COMMITTEES:
Appropriations

Attachment 1
Jan 21, 2019
Page 1

To: Chairman George Keiser and Members of the House Industry, Business and Labor Committee

Date: January 21, 2019

Support Testimony for HB 1524

Good afternoon, Mr. Chairman and members of the committee. My name is Corey Mock, representative from District 18 in Grand Forks, and one of the sponsors of House Bill 1524.

I'm going to begin by offering an amendment of the bill, followed by an explanation and proposal. The amendment I've distributed is a hoghouse amendment that will replace all policy language with an optional legislative management study to be conducted this interim.

HB 1524 was introduced as a first draft and placeholder for a much larger and more important conversation. Data privacy is a growing concern around the world, and rightfully so. Facebook was estimated to own the world's largest database of people ever built -- and that estimate was made six years ago when they reported approximately 1.2 billion active users. Today, Facebook has nearly twice the number -- 2.23 billion active users – on their platform.

Here's what we know about those users as of September 18, 2018:

- 1.57 billion people accessed Facebook daily from a cell phone;
- 1.47 billion logged into Facebook daily from a desktop computer;
- 53% of users are female and 47% are male;
- Globally, 83% of women and 75% of men use Facebook;
- 72% of online users with an income more than $75,000 per year are on Facebook;
- Average Facebook user has 155 "friends;" and
- Americans spend 58 minutes per day on Facebook.

HB 1524

Attachment 1
Jan 21, 2019

Facebook is one of many free social media tools and apps that collect data on users on a regular basis. As the saying goes, "if you're not paying, then you're the product." Software owners analyze and sell user data that is often used by advertisers. Everything from age, interests, purchasing habits, location history, health, and social statistics are all data collected, often in the background when apps are not being used.

One example of an application collecting unnecessary data is a flashlight app that turns on the LED flash of mobile phones. This simple app that only needs to control one function of the phone had access to calendars, location, and camera. One of these apps were addressed in a case before the Federal Trade Commission in 2013, but there are numerous examples where the only solution is due diligence by the end user.

There are also several cases where apps are collecting and storing information that you agree to, but are not protecting or encrypting the data properly. In 2014, Starbucks was found to be storing passwords, email addresses, and previous GPS information without encryption. They quickly corrected the error once it was discovered, but not all companies have been diligent in taking necessary precautions.

Currently there are no comprehensive data regulations in the United States. In 2016, the European Union passed the General Data Protections Regulation (GDPR) with complete rollout completed in May 2018. Without going into details, GDPR regulates the collection, storage, and sale of data, including names, images, email addresses, social media posts, medical information, IP addresses, and bank information. To be clear, GDPR does not prohibit the collection of data, but requires companies to adhere to specific standards and can impose steep penalties on any company with an electronic presence in the European Union.

California also passed comprehensive data regulation policies in 2018 -- the California Consumer Privacy Act (CCPA). CCPA affords California residents with an array of new rights, beginning with the right to know what information companies have collected and why. It also allows consumers to request the deletion of personal information, ability to opt-out of data sharing, and access their personal information in a readily useable format.

This committee will have a separate conversation about consumer data privacy during the hearing of Rep. Jim Kasper's proposed legislation: HB 1485.

HB 1524

Attachment 1
Jan 21, 2019

The bill before you was based on legislation adopted by the state of Vermont in the summer of 2018. This legislation seeks to define "data brokers," companies who knowingly collect and sell consumer information to third parties. This legislation requires data brokers to register with the Secretary of State's office, develop a comprehensive information security program, and gives the Attorney General jurisdiction to enforce requirements outlined in this section.

While I'm unaware of anyone specifically here to testify in support of HB 1524 in it's current form, I do know that several companies are likely going to oppose the policies laid out before you.

To be clear, the intention of HB 1524 is to begin a much-needed conversation and hopefully develop comprehensive data privacy regulations that define terminology, identify state, corporate, and consumer responsibilities, and provide basic assurances to North Dakotans that all public and private entities operating in our state are treating personal information they collect with the respect it deserves.

If the committee is willing, I would recommend the committee take testimony on HB 1524 and accept the proposed amendment as an option of last resort. Hold this bill and, following the hearing of HB 1485, appoint a subcommittee that can work with concepts and language from both bills while soliciting input from industry and consumer advocates alike.

Sponsors of HB 1524 are willing and eager to work with Rep. Kasper and his co-sponsors, as well as members of the committee and interested parties, to develop a single policy that can be a role-model for other states to adopt -- without unnecessary or technology-restrictive regulations.

If the committee would prefer, I would be happy to return for the hearing of HB 1485 and answer questions of this bill so committee members can evaluate details of both data privacy bills at the same time.

Thank you again for your work and consideration of current and future amendments, should they be necessary.

FOR SOME PEOPLE, THE VERY IDEA IS MORTIFYING

HB 1524

Attachment 1
Jan 21, 2019
Page 4

future tense

How to Understand What Info Mobile Apps Are Collecting About You

It takes a little work, but it's worth it.

By LISA GUTERMUTH
FEB 24, 2017 • 11:01 AM

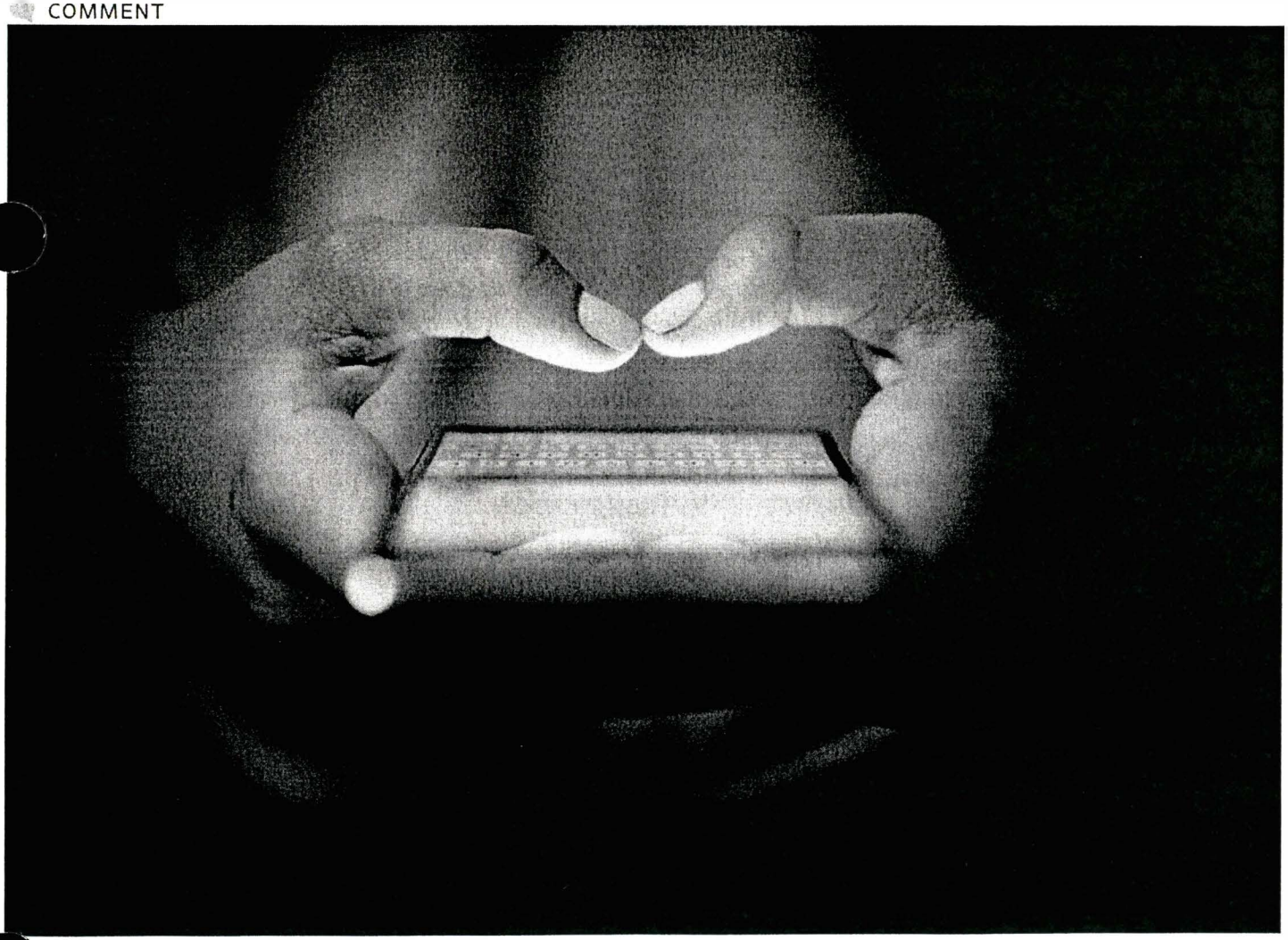


Photo illustration by *Slate*. Photo by Diego Cervo/Thinkstock.

Attachment 1
Jan 21, 2019
pg 5

HB 1524

There's an old truism that's popular among privacy advocates: "If you're not paying, you're the product." Your age, interests, purchasing habits, frequented locations, health, and social map are all valuable pieces of information that comprise a digital shadow, which can be packaged, bundled, and sold to the highest bidder.

It's tempting to download the coffee shop app so you can have the convenience of ordering ahead. Figuring out what data that app is collecting, on the other hand, can be awfully inconvenient. But many apps engage in irresponsible practices that are worth understanding. Once you know how to spot them, you can decide which apps are worth the potential invasion of privacy, and which should be banished from your devices forever.

Apps that collect way more information than is necessary—and sometimes share and sell it

Take flashlight apps. They're meant to do one simple thing: turn on the LED flash of mobile phones. But many ended up having access to a lot of unnecessary data and phone functions, including users' calendars, location, and camera. The infamous "The Brightest Flashlight" app shared users' precise location and unique device identifier to third parties without disclosing that it did so—not exactly critical to a functioning flashlight. The Federal Trade Commission addressed this case in 2013, but there are plenty of other examples where this is not the case. Be wary of the cartoon game that wants to access your personal photos, or the weather app that requires access to your microphone. Uber, for instance, requires access to your location data even when you are not using it unless you turn off location data entirely on your phone.

That's because information collected by apps is frequently shared with and sold to third parties. This is usually disclosed in the privacy policy, if the app actually has one. According to a 2016 Future of Privacy Forum study, at least 24 percent of top apps still do not have a privacy policy. While there is a wealth of literature about how terms of service agreements and privacy policies are not often read, they are still critical features as they spell out company commitments and are legally enforceable. One bit of good news: Google plans to remove apps that handle personal or sensitive data from the Google Play Store if they don't have privacy policies. (You can get more

information about companies' disclosures and commitments regarding privacy from Ranking Digital Rights, a New America project I work for.)

HB 1524

Attachment 1
Jan 21, 2019
pg 6

Apps that pull you into their greater ecosystem

First, ask yourself what the added value of having an app is: Plenty of people use Facebook and other services on their mobile devices, for example, without having an app. Downloading an app provides companies with more direct access to your information than a visit to their website will. Prime examples of this are the Facebook and Messenger apps. You can access Facebook from your mobile browser, but once you try to use the messaging feature there, you'll be out of luck—you're forced to download Messenger. As the *Guardian* put it: "The real reason that Facebook is pushing chat into its Messenger is to create another platform or silo from which Facebook can access you as a user."

Apps that don't protect your data

In 2014, the Starbucks app was found to be storing passwords, email address, and previous GPS information unencrypted, leaving it open to onlookers to exploit. Starbucks addressed this vulnerability shortly after it was discovered, but it is certainly not the only app to have had this issue. More recently, *Wired* conducted an investigation into the top 10 dating apps in the United Kingdom and found that most had some insecurity that leaked personal information of the users. This is also something that you can look out for in privacy disclosures (when they exist), which should spell out a company's commitment to using strong encryption in both storage and transmission of personal data. If you can't find any language to that effect, don't use it.

* * *

You may be tempted to just give up and let all your data hang out. But you can take control of your information. Here are four steps you can take right now to better improve your digital autonomy through your mobile device, inspired by the MyShadow project—which has worked for years to promote awareness around digital shadows and what users can do about them.

1. Take control and change your settings.

Apple iOS gives you a clear, useful overview of which apps have access to different types of data; you can find it by going to Settings > Privacy.

Android version 6.0 (Marshmallow) and up also enables users to manage app permissions by going to Settings > App > Permissions. Turn off permissions to data tracking when they are not in use. For example, ride and map apps don't need to have access to your location data when you're not actively using them. (Bonus: Turning these permissions off will also save on battery power.)

Attachment 1
Jan 21, 2019

2. Check disclosures.

If you're not going to read the privacy policy, at least make sure the app *has* one. And if you're concerned about your financial, fitness, health, or other sensitive information being secure, then check to see how seriously the app maker takes encrypting user data by looking at their disclosures in the privacy policy, which should be located at the bottom of the page in the app store before you download.

3. Use apps that maximize your privacy.

Signal is a secure messaging app that uses end-to-end encryption to protect your texts and voice calls. DuckDuckGo is a search engine that explicitly does not collect, store, or share any information about you. Disconnect is also an app that seeks to protect users from tracking and improve device performance. These apps clearly state in their privacy policies what information (if any) they must collect in order for the app to function and that they do not share this information with any third parties unless legally bound to do so. Signal may not have stickers for your photos, but it's a lot more secure.

4. Perform regular app maintenance.

This means regularly updating your apps, checking permissions, and deleting unused apps. Updates are usually good things, because they come with new security features and improvements. However, when apps are updated, they can often access different data and in different ways. What's more, many apps, through security bug or design, collect data even when the app is dormant. The Norwegian Consumer Council recently performed an app audit that highlighted how often this happens. If you haven't used an app in over a month and can easily download it again should you need it in the future, bin it.

This article is part of the cybersecurity self-defense installment of Futurography, a series in which Future Tense introduces readers to the technologies that will define

How Facebook Sells Your Personal Information

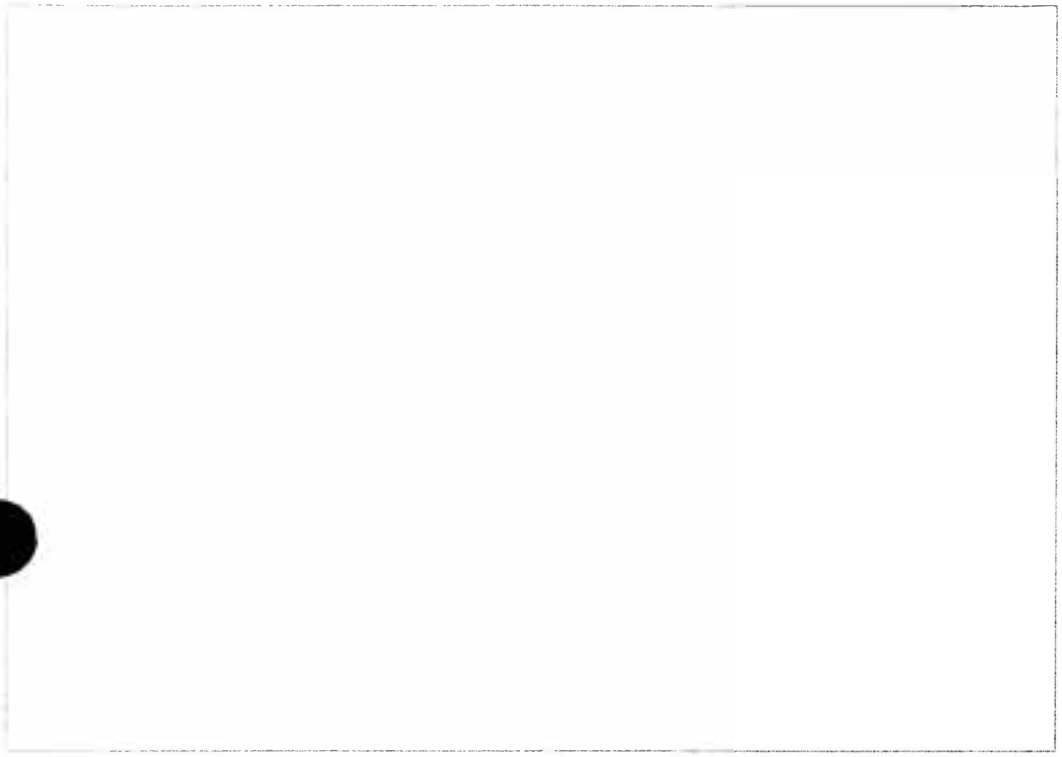
pg 8

Facebook expects personal data sharing to double every decade and plans to target members' information more closely.

HB 1524

Attachment 1
Jan 21, 2019

BY DNEWS
PUBLISHED ON 01/24/2013
2:26 PM EST



Now that Facebook has gone public and is struggling to get a steady valuation, the company is looking to find new ways to make its money and prove its worth to investors.

One option Facebook is exploring is enhancing ad sales by more effective targeting of increasingly specific demographic groups, using location data from mobile devices and information culled from the site.

The company will be targeting members' information more closely, and expects personal data-sharing to double every decade.
ANALYSIS: Now You Can Stay Social While Showering

That forces Facebook members to consider just how much of their personal information to share, both now and in the future.

How might Facebook's already flexible privacy policy change as the company works harder to become a platform for engaging with brands? How will that affect the end user?

Marketing Treasure Trove We have to start by taking a look at the data in question. How much of a danger to the consumer is the data that Facebook has? Exactly how much data does it really have?

Peter Pasi, executive vice president at Emotive LLC, an Arlington, Va.-based firm that focuses on digital outreach for political campaigns, says Facebook has quite a bit.

Attachment 1
Jan 21, 2019

"Facebook is the largest opt-in community of individuals in the world, and boasts unparalleled reach," Pasi said. "In English, that means it's likely the largest database of people ever built, and contains more personal data than any other source."

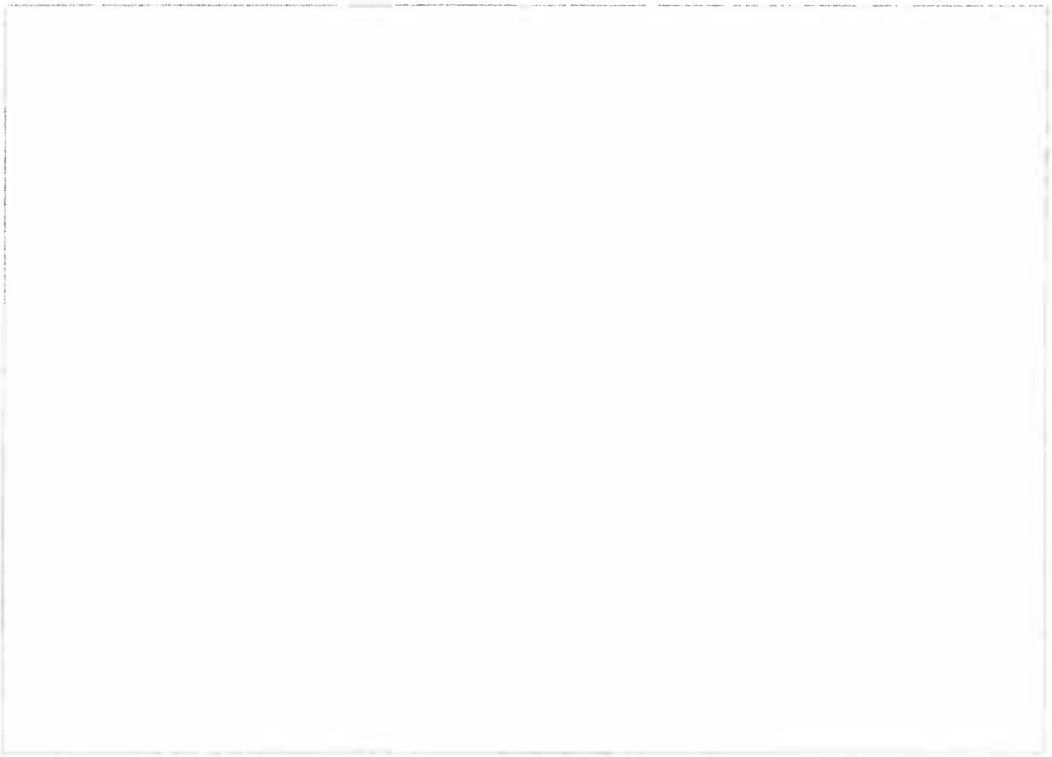
We know that Facebook has a lot of information about us, both what we enter ourselves and the data that our friends choose to put up about us.

ANALYSIS: Social Media More Addictive than Booze

Remember the last time your friends tagged you at a location and posted photos? They were sharing your personal data with Facebook. [10 Ways to Protect Yourself on Social Media Websites]

What Marketing Companies Look For, and How Much They Can Use "Online marketers look at signals," Pasi said. "Did someone visit a snowboarding vacation site, or put a new snowboarding jacket in their online shopping cart and not buy it? Have they been searching for snowboarding equipment? These are the types of things that signal a marketer that a consumer is interested in, or intent on, making a purchase."

You can see how quickly information that seems innocuous when you post it on Facebook can make you a target for specific marketing goals.



Facebook recently announced the limited beta release of Graph Search, a feature that will create a new way for people to navigate connections and search social networks. | Josh Edelson/AFP/Getty Images

Location tagging is, in and of itself, another way to make you an attractive target to marketers. You're giving away information about which brick-and-mortar retailers you are likely to frequent, allowing for even more enhanced targeting.

Attachment 1
Jan 21, 2019

So what are the limits when it comes to Facebook sharing members' personal data with advertisers and marketers? Do regulations prevent any of this sharing at all?

[redacted]e issues are really being formed right now, said Allison Hobbs, an intellectual-property and copyright lawyer in New York.

TOP 10 Social Networking Sites

"Social media companies should not engage in deceptive or unfair trade practices," Hobbs said. "As far as end-user data is concerned, that means social media companies should honestly disclose what they plan to do with it. Usually, they do this through their Terms of Service or privacy statements.

"When they are not honest, the Federal Trade Commission, which regulates deceptive and unfair trade practices, may issue a complaint against them," Hobbs said. "In 2011, the FTC issued complaints against Google and Facebook; the result was that both parties are required to do privacy audits until 2032.

"So, it looks like the issue is being handled on a case-by-case basis, which may result in better rules than legislation or prophylactic regulation, since it is more likely to keep up with technological change."

Gaining Perspective What can you do to help keep your personal data from becoming a marketing director's dream?

The best thing is to look at the data that you share on Facebook, and the data that your friends share about you, and take control over it all.

[redacted]NALYSIS: Footwear Meets Social Networking

Ask your friends not to tag you in any of their posts. When you find yourself in an unwanted photo, remember that you can always untag yourself.

You should always carefully read through any changes to Facebook's privacy policies. If worse comes to worst, you may have to decide whether you want to keep using Facebook at all.

Get More from TechNews Daily

11 Facebook Privacy Steps to Take Now Got Money? You're a Prime Target for Identity Thieves 10 Best Social Networking Websites This article originally appeared on TechNewsDaily.

HB1524

pg 11
Attachment 1
Jan 21, 2019

Your Smartphone and Its Apps Can Track You

VIDEO REVIEW SCIENCE IO9 FIELD GUIDE EARTHER DESIGN PALEOFUTURE

David Nield
1/04/18 12:27pm •

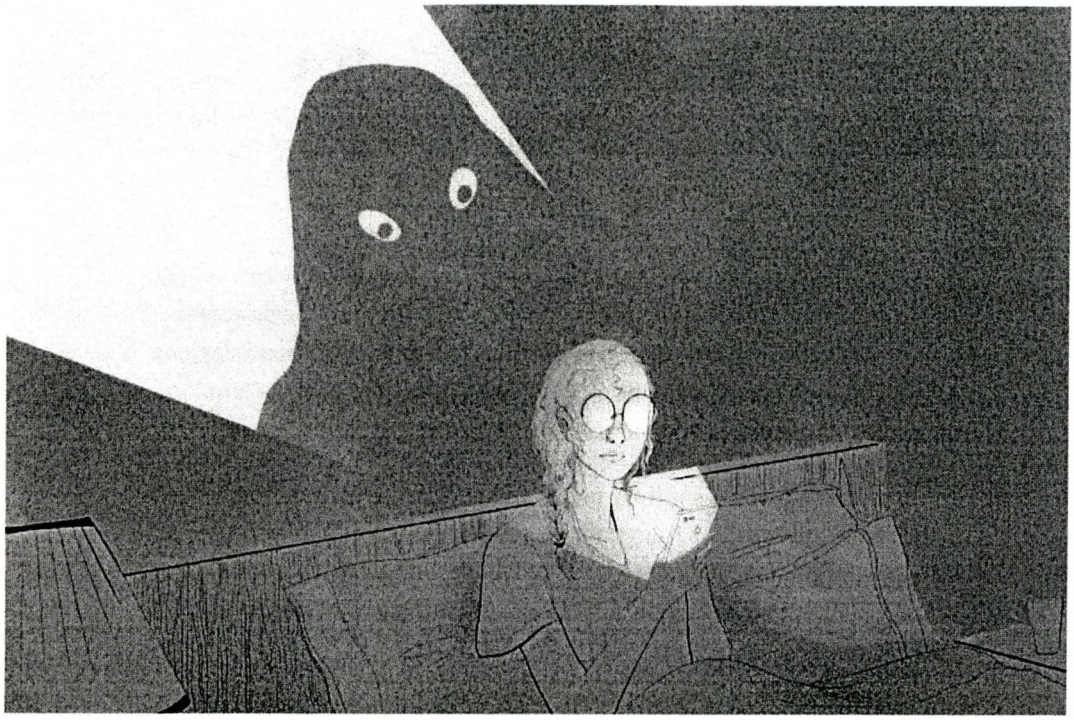


Illustration: Chelsea Beck/GMG

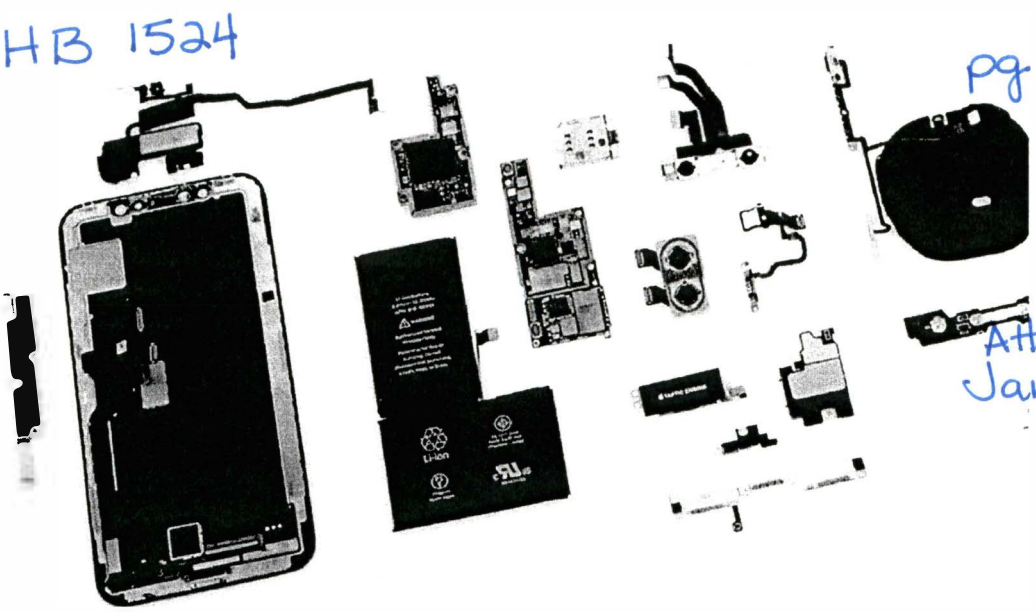
The little pocket supercomputers we all constantly carry around with us aren't just supplying us with useful information, they're also collecting a host of data on us and our habits, all of the time. Here's a guide to what gets collected by your smartphone and the apps running on it, and how you can take back some control.

Sensors, Android, and iOS

Your smartphone is packed with sensors, monitoring where you are in the world, how fast you're moving through space, which way up you're holding your phone, and more. All of this data is used by apps to improve the user experience—so making sure your phone apps switch between landscape and portrait modes, and keeping you on the right route for your commute—but how much of this data is logged and stored is largely up to the choices of the handset manufacturer.

In recent months OnePlus has been at the center of a privacy kerfuffle over the way it was logging personally identifiable information (like device IDs) and transmitting that data back to OnePlus's home base, ostensibly to improve the device's user experience. OnePlus has since dialed back some of that data collection, and promises to only use the data it gathers internally, but it shows just how much data your smartphone can reveal, and how tricky it can be to know what's being collected and what isn't.

HB 1524 pg 12



Attachment 1
Jan 21, 2019

Image: iFixit

Google's privacy policy, which affects Android among other services, is here: You can see that as soon as you sign into Android with your Google account, your device gets linked to your Google credentials, and Google starts logging data such as the length and type of your phone calls, your phone's location, the device you're using, and more.

You can also find Apple's privacy policy online. While a lot of the data collected is the same, Apple differs from Google by making much of it anonymized or kept on your iPhone (and not sent back to Apple)—so while your location can be tracked on iOS, for example, Apple itself doesn't know where you are, only your phone does.

Face ID is another good example of how Apple differentiates itself on privacy. The Face ID sensors map and know everything about your face, but that information is then stored privately and securely on your phone—it isn't transferred back to Apple or iCloud, making it very difficult for anyone to get a copy of your face.

However, some of this data is shared with third-party apps. For example, some app might want to stick an AR filter on your face. Apple requires that any app requesting such face-scanning features must present a privacy policy to the user.

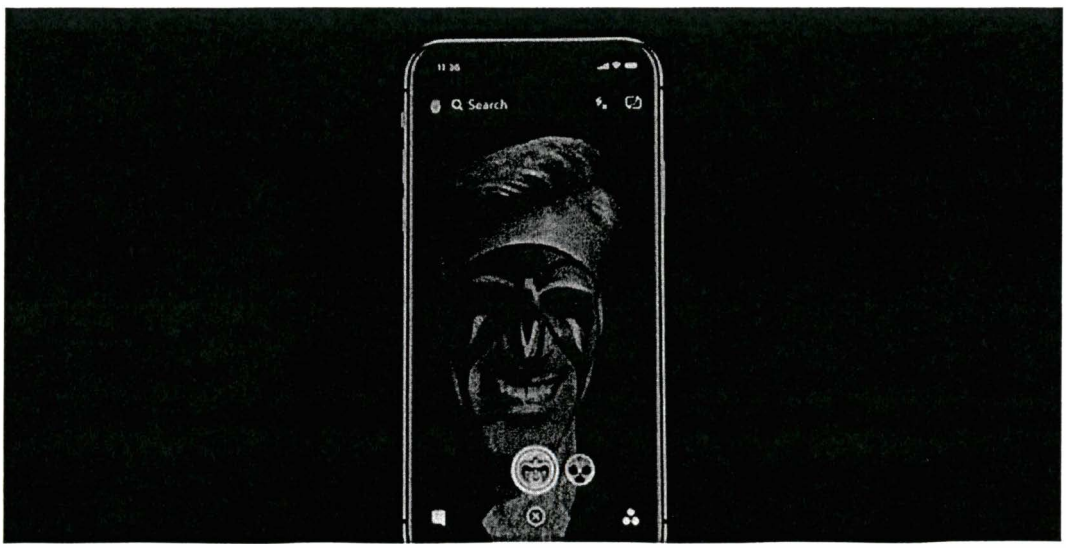


Image: Apple

HB 1524

Attachment 1
Jan 21, 2019
pg 13

Smartphone apps

On top of the basic information collected by your smartphone and beamed back (or not beamed back) to the company that made your handset, there's all the information collected by the apps you run too—the data that gets recorded and saved is down to an individual app's privacy policies and the permissions you give it.

If you want to know exactly what an app is allowed to track on your Android phone, open the Settings app then go to **Apps & notifications**, choose an app, and select **Permissions**. Over on iOS, launch the Settings app then pick an app to see the permissions it has. Most of these permissions can be revoked with a toggle switch on both Android and iOS.

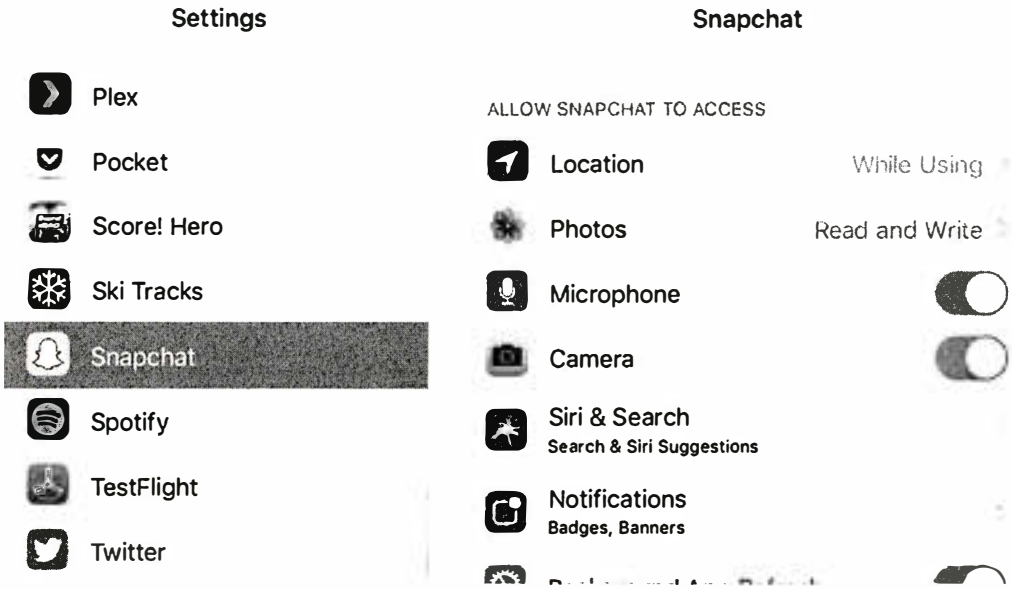


Image: Screenshot

That tells you the specifics of the data an app can track on your phone, but to know exactly how that data is being used, you need to dig down into that app's terms and conditions of use and privacy policy, if the app even has one. Google recently said it would be cracking down on apps without user data policies, but you're still largely at the mercy of app developers in terms of how your data gets used.

For example, you can read the Airbnb privacy policy here. Using the app on your phone? Airbnb can track your location, get information about the device you're using, and log the times you use the app. This data is then used for everything from showing you Airbnb venues near your current location, to better targeting listings to you.

Even when you think you know what's being tracked, it's not always clear cut: Developer Felix Krause recently revealed how granting an app permission to see photos on your device also lets that app see where you've been, because all of your pictures have geotags on them by default. Even if you're blocking an app from tracking your location, it can probably still work out where you live

and where you go on holiday most often through your stored pictures. Of course, whether the app actually will harvest this data for whatever purpose is again up to the developer.

Just when you think you know what an app is and isn't tracking, you find out that Uber was secretly recording iPhone screen activity, supposedly to improve functionality with the Apple Watch app. If you want to take Uber's word for it, the feature was used to do the job of map rendering on the phone before transferring it to the wearable, but it's another example of just how in the dark end users can be.

Image: Screenshots

Head to the web in your mobile browser of choice and all the data we've previously talked about being collected online comes into play again here—your searches, the device you're on, where in the world you are, and so on. There are two layers to the tracking: the data tracked by your browser app, and the data tracked by the sites you visit.

Again, that's down to the apps and the services you're choosing to use. Google Chrome, you might not be surprised to know, logs a ton of data, including your browsing history and thumbnails of the sites you visit, and of course if you sign in with Google too then all of your activity feeds back into your Google profile by default. Safari tracks a lot of the same data as well, though in line with Apple's policies it keeps much of it saved locally on the device, and now includes tracking blocking tools for stopping advertisers from following your browsing behavior across the web.

Taking back control

As you can probably tell, getting a handle on exactly what data is collected, and then how that data might be used or passed on to third-parties, isn't easy—these policies are couched in ambiguity to give the manufacturers plenty of leeway. Samsung, for instance, as per its policy, might collect GPS information from your phone, might pass your voice searches on to a third party for speech-to-text conversions, and might share all this data with business partners who might use it to advertise to you.

Image: Screenshots

That's a lot of mights and maybes. Ultimately, if you don't like the deal, you don't use the phone. But there are certain settings on your handset you can use to block devices and individual apps from harvesting as much data as they'd perhaps like to.

Location tracking is a big one—very valuable to both end users and advertisers alike. On (stock) Android you can disable location tracking on the device as a whole by opening Settings, then tapping **Security & location** and **Location**, and then turning tracking off. On iOS, open Settings, then go to **Privacy** and **Location services**, and disable the feature. From the same menus you can turn off or limit location tracking on an app-by-app basis.

We've already spoken about editing individual app permissions, either through the **Apps & permissions** menu in Android Settings, or by tapping on an app name in iOS Settings. Most of these permissions are self-explanatory, such as access to your calendars and contacts, but you can also control whether or not apps can pull data from the motion sensors in your phone (for counting steps and so on)—this is labelled **Body sensors** in Android and **Motion & Fitness** in iOS.

HB 1524

Attachment 1
Jan 21, 2019
Pg 16

As far as Google is concerned, you've got a whole host of options to manage, covering Google's apps on Android, iOS, and everywhere else. If you open up your Google account page on the web, then pick **Personal info & privacy**, it's possible to change the way data is collected (via **Go to Activity Controls**) or erase some of the data Google already has on you (via **Go to My Activity**). For instance, you can see and erase all the voice searches that you've run through Google Assistant on your phone.

Image: Screenshot

Individual apps may have specific settings and privacy options you can take advantage of, though most won't, and few app developers will be as interested in collecting data about you as Google. Facebook is one exception, and we've written before about how Facebook follows you across your devices and how you can limit this to some extent.

In the end your smartphone use is helping to build up a picture of who you are and the kind of advertising you're interested in for companies like Google, Facebook, and others—even if an app isn't part of a massive advertising network, it may well sell its data to one. Apple stands apart in this regard, keeping the data it tracks for its own use and largely on a single device, though of course the apps that run on iOS have more freedom to do what they want.

Even if you're reasonably content to put up with some monitoring on Android and iOS, it's important to know what kind of data you're giving up every time you switch your smartphone on. Whether it means you uninstall a few social media tools, or disable location tracking for a few apps, it gives you some semblance of control over your privacy.

This story was produced with support from the Mozilla Foundation as part of its mission to educate individuals about their security and privacy on the internet.

HB 1524

Inside Privacy

Updates on developments in data privacy and cybersecurity

FROM COVINGTON & BURLING LLP

pg 17

COVINGTON

Attachment 1
Jan 21, 2019

Vermont Publishes New Guidance on Law Regulating "Data Brokers"

By James Strawbridge on December 21, 2018
Posted in Data Privacy

On December 11, 2018, the Vermont Office of the Attorney General published **new guidance** on the state's data broker law (**Act 171 of 2018**), which imposes new data breach notification requirements on "data brokers" and takes effect on January 1, 2019. The new guidance clarifies the definitions of key statutory terms and the scope of the law's various requirements.

Definition of "Data Broker": The law defines "data broker" as a business or business unit "that knowingly collects and sells or licenses to third parties the brokered personal information of a consumer with whom the business does not have a direct relationship." The new guidance suggests that many businesses are not covered by the law. For instance, the new guidance notes that "an application, website, or social media platform that sells information about its users is not a data broker" because those businesses have a "direct relationship" with users. Similarly, because "data brokers" must "collect" and "sell or license" data, "[a] business that acquires lists of individuals in order to market to them or customize their product offerings, but does not resell the data, is not a data broker." On the other hand, "a business that collects information about consumers and then adds additional data elements, cleans up the data, or categorizes the data into lists in order to sell or license the data ... is a data broker."

Definition of "Brokered Personal Information": The law defines "brokered personal information" as "one or more" of a list of "computerized data elements about a consumer, if categorized or organized for dissemination to third parties," as well as "other information that ... would allow a reasonable person to identify the consumer with reasonable certainty." 9 V.S.A. § 2430(1). The guidance explains that, because "brokered personal information" must be "categorized or organized for dissemination," the business possessing the data "must have done something to the data to prepare it for dissemination" in order for it to be implicated under the law. Accordingly, "[d]ata that is stored in a business's databases for internal use by that business, with no intention of disseminating outside the business," does not constitute "brokered personal information" under the law.

Scope of Data Broker Obligations: Businesses that qualify as "data brokers" must register with the Vermont Secretary of State annually and provide certain information. For instance, if a data broker permits consumers to opt out of its collection, sale, or storage of their information, it must detail the method for requesting such an opt-out. The new guidance clarifies, however, that the law "does not require a business to permit consumers to opt out of its collection, sales, or storage of their information, if that is not its practice." The guidance also notes that data brokers must track and report to the Secretary of State annually the number of security breaches they experience during the prior year and, if known, the number of Vermont consumers affected.

Data Security Standards: The law requires data brokers to maintain certain data security standards in order to protect consumers' personally identifiable information. The new guidance stresses that "critical elements" of these new security requirements include that data brokers maintain a written security program; perform a risk assessment; track employee compliance with policies and procedures; implement measures that prevent terminated employees from accessing personally identifiable information; and review the scope of security measures at least annually.

HB1524

Attachment 1
Jan 21, 2019
pg 19

Analysis: Vermont's data broker regulation

Jul 11, 2018 Save This ()

Hawah Ahmad, CIPP/E Hawah Ahmad, CIPP/E

The Vermont state legislature recently enacted a first-of-its-kind bill to regulate data brokers — without the signature of its governor, Phil Scott (https://www.burlingtonfreepress.com/story/news/politics/government/2018/05/22/gov-scott-vetoes-four-bills-including-15-minimum-wage/634966002/).

Following the Equifax data breach, and motivated by a December 2017 report (https://vermontbiz.com/news/2017/december/18/ag-wants-vermont-be-first-data-broker-regulator) from the Vermont attorney general and Department of Financial Regulation, H.764, An act relating to the regulation of data brokers (https://legislature.vermont.gov/assets/Documents/2018/Docs/ACTS/ACT171/ACT171%20As%20Enacted.pdf), ultimately extends to data brokers requirements for information security programs similar to those mandated by the Gramm-Leach-Bliley Act (https://iapp.org/resources/topics/the-gramm-leach-bliley-act/) and the Security Rule of the Health Insurance Portability and Accountability Act (https://iapp.org/resources/topics/hipaa/).

Definition of data broker

The law narrowly defines the term "data broker" as "a business or unit/s of a business, separately or together, that knowingly collects and sells or licenses to third parties the brokered personal information of a consumer with whom the business does not have a direct relationship." To meet the criteria of a data broker, the individual must sell or license brokered personal information which is comprised of one or more computerized data element such as name, address, date or place of birth, mother's maiden name, biometric data and the like, as well as "other information that, alone or in combination with the other information sold or licensed, would allow a reasonable person to identify the consumer (with reasonable certainty) to a third party."

An important limitation on the definition of "data broker" is that the law doesn't apply to businesses that collect information from their own customers, employees, users or donors, or to businesses that "provide services for consumer-facing businesses and maintain a direct relationship with those consumers, such as a website, 'app,' and e-commerce platforms."

Consumer protection requirements

The law applies four approaches to ensuring consumers' protection: prohibiting the acquisition and use of data for fraudulent purposes; increasing transparency through registration and disclosure; freeing consumers from monetary deterrents; and providing for minimum information security requirements.

Prohibition on data use

The Vermont law prohibits the acquisition of brokered PI by fraudulent means and the acquisition and use of brokered PI for the purpose of stalking or harassment, committing fraud (e.g. identity theft, financial fraud, or e-mail fraud), or to engage in unlawful discrimination (including but not limited to employment and housing discrimination).

Transparency

Annual registration: Under the law, data brokers who sell or license "brokered personal information" must pay $100 and register annually with the Vermont Secretary of State by January 31 following a year in which a person meets the criteria for being a data broker.

Disclosures to consumers: Additionally, upon filing, a data broker must provide consumers with the name and primary physical, email and internet addresses of the data broker, how to opt out of first-party and third-party data collection, whether the data broker implements a purchaser credentialing process, and if the business experienced any security breaches within the last year along with the number of individuals affected by breach. Data belonging to minors is subject to additional disclosure requirements.

Freedom from monetary deterrents

Vermont's new law separately requires credit reporting agencies, not data brokers, to offer consumer credit security freezes and unfreezes free of charge. Consumers can already receive their credit report free once per year from each of the three major credit reporting agencies. Additionally, the law requires higher security requirements for authentication to be able to initiate or lift a credit freeze. This law also creates a one-stop shop for credit freezes in which a credit freeze with one credit reporting agency is required to initiated freezes with other credit agencies.

Requirement for information security program

Data brokers are required to develop, implement, and maintain a comprehensive information security program that is written, readily accessible and able to protect personally identifiable information with administrative, technical and physical safeguards appropriate the scope and size of the business. Requirements include:

- Designation of employees to maintain the program.
- Privacy risk assessments for reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of any electronic, paper, or other records containing personally identifiable information, with a process for evaluating and improving the effectiveness of the current safeguards for limiting such risks.
- Record keeping for disciplinary measures for violations of the comprehensive information security program rules.
- Data minimization and limited employee access to records.
- Management of third-party vendors.
- Regular monitoring, review, and update the security program.
- Documenting actions taken in response to security breaches and post-incident reviews.

Additionally, the minimum requirements for the information security program should include computer system requirements for secure user authentication protocols including access controls, secure password requirements, encryption or protocols with a higher degree of security, reasonable monitoring of unauthorized access or use of personally identifiable information, and up-to-date system security software and training for employees. The attorney general may adopt rules to implement the new security provisions.

Enforcement

pg 21

H.764 provides a layered effective date in which the findings and intent of the law, elimination of fees for placing or removing a credit freeze, and future report requirements went into effect immediately following its passage. However, data brokers will have until January 1, 2019, to comply with the annual registration, technical requirements and disclosures to consumers as presented in Chapter 62.

Enforcement of data broker registration is regulated by the Attorney General's Office and can result in civil penalties, action in the Civil Division of the Superior Court to collect penalties, and appropriate injunctive relief. Failure to meet the new security program requirements can be declared "unfair and deceptive act[s] in commerce." Lastly, an enforcement action must be brought by both the Attorney General. However, private citizens can seek civil action under credit reporting laws.

Pease International Tradeport, 75 Rochester Ave, Suite 4
Portsmouth, NH 03801 USA • +1 603.427.9200

HB 1524

Attachment 1
Jan 21, 2019

HB 1524

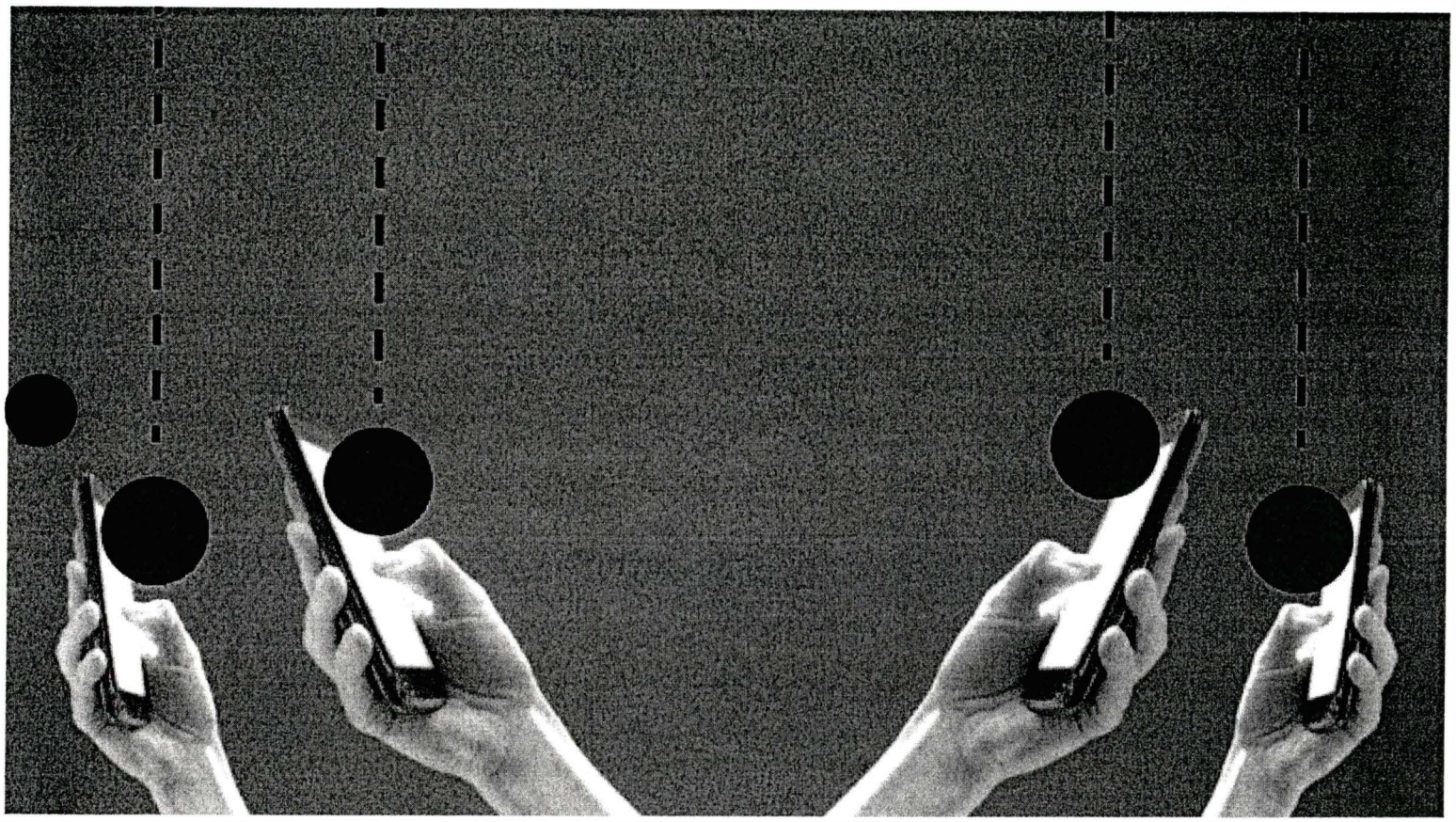
Attachment 1
Jan 21, 2019
pg 22

[redacted]LATION

What You Need to Know About California's New Data Privacy Law

by Dipayan Ghosh

JULY 11, 2018



pm images/Getty Images

Late last month, California passed a sweeping consumer privacy law that might force significant changes on companies that deal in personal data — and especially those operating in the digital space. The law's passage comes on the heels of a few days of intense negotiation among privacy advocates, technology startups, network providers, Silicon Valley internet companies, and others. Those discussions have resulted in what many are [redacted]bing as a landmark policy constituting the most stringent data protection regime in the United States.

Much of the political impetus behind the law's passage came from some major privacy scandals that have come to light in recent months, including the Cambridge Analytica incident involving Facebook user data. This and other news drove public support for a privacy ballot initiative that would have instituted an even stricter data protection regime on companies that deal in consumer data if the state's residents voted to pass it in Novem But after intense negotiation, especially from leading internet companies and internet service providers, the backers of the ballot initiative agreed to drop the initiative and instead support the passage of the law.

The new law – the California Consumer Privacy Act, A.B. 375 – affords California residents an array of new rights, starting with the right to be informed about what kinds of personal data companies have collected and why it was collected. Among other novel protections, the law stipulates that consumers have the right to request the deletion of personal information, opt out of the sale of personal information, and access the personal information in a "readily useable format" that enables its transfer to third parties without hindrance.

The law notably establishes a broad definition of "personal information," drawing in categories of data including a consumer's personal identifiers, geolocation, biometric data, internet browsing history, psychometric data, and inferences a company might make about the consumer. The protections over this data are to be enforced by the state's attorney general, though consumers will maintain a private right of action should companies fail to maintain reasonable security practices, resulting in unauthorized access to the personal data. (The data breach protection applies to a set of personal data that is narrower than that protec in the more general privacy protections.)

Perhaps the primary issue that firms are contending with is that the law's requirements could threaten established business models throughout the digital sector. For instance, companies that generate revenue from targeted advertising over internet platforms – such as Facebook, Twitter, and Google – must, as the law is currently written, allow California residents to delete their data or bring it with them to alternative service providers. This restriction could extend to internet service providers such as AT&T and Verizon, which collect broadband activity data (web browsing data) and could attempt to use it to generate behavioral profiles to enable digital advertising. These measures might significantly cut into the profits these firms currently enjoy, or force adjustments to their revenue-growth strategies. They could also further impact any businesses that advertise on digital platforms, as the service they are purchasing – highly targeted advertising – might become less precise as a result of the new protections afforded to individual consumers.

Some firms stand to lose even more. Data brokers such as Acxiom, Epsilon, Experian, and Oracle, for example generate profits by collecting quantities of data on individual consumers and selling it to third parties – be ad networks, marketers, retailers, or any other type of interested business. These are precisely the kinds of practices that are directly threatened by the consumer's rights to deletion and to opt out of sale of data.

While the law, which is set to come into effect at the start of 2020, technically applies only to California residents, it will most likely have much broader implications. Most major companies that deal in consumer data, from retailers to cellular network providers to internet companies, have some Californian customers. That leave those companies with two main options: either reform their global data protection and data rights infrastructures to comply with California's law, or institute a patchwork data regime in which Californians are treated one way and everyone else another. That last option can be more expensive for companies, and could disgruntle non-Californian customers should they be given fewer data privacy options by the service provider. Indeed, similar questions about Americans' data rights arose during Mark Zuckerberg's congressional testimony in regard to Facebook's compliance with new European regulations.

Critically, the legislature has left open the door to amendments to the new law. We can also expect the state attorney general to work with public stakeholders to develop more specific compliance guidance for the industry over the months ahead. In the time before the law is enforced, we are likely to see more debate among industry leaders, consumer advocates, and everyone in between — all of whom will wish to affect the law and its enforcement to their own benefit.

HB 1524 Jan 21, 2019 Attachment 1 pg 24

Dipayan Ghosh is a Fellow at New America and the Harvard Kennedy School. He was a technology and economic policy advisor in the Obama White House, and formerly served as an advisor on privacy and public policy issues at Facebook. Follow him on Twitter @ghoshd7

This article is about REGULATION

⊕ FOLLOW THIS TOPIC

Related Topics: TECHNOLOGY | SECURITY & PRIVACY | ADVERTISING, MARKETING & PUBLIC RELATIONS | TECHNOLOGY

Comments

[redacted] a Comment

POST

Attachment 2

19.1041.01001
Title.

Prepared by the Legislative Council staff for
Representative Mock
January 21, 2019

PROPOSED AMENDMENTS TO HOUSE BILL NO. 1524

Page 1, line 1, after "A BILL" replace the remainder of the bill with "for an Act to provide for a legislative management study of privacy practices in the data broker industry.

BE IT ENACTED BY THE LEGISLATIVE ASSEMBLY OF NORTH DAKOTA:

SECTION 1. LEGISLATIVE MANAGEMENT STUDY - DATA BROKER INDUSTRY. During the 2019-20 interim, the legislative management shall consider studying privacy practices in the data broker industry to determine whether adequate safety measures exist to prevent fraud and protect the identifying information of consumers. The study must include consultation with the department of commerce and the attorney general, and an evaluation of the nature and sources of the consumer information the data brokers collect, how data brokers use, maintain, and disseminate the information, and the extent to which the data brokers allow consumers to access and correct their information or to opt out of having their personal information sold. The legislative management shall report its findings and recommendations, together with any legislation required to implement the recommendations, to the sixty-seventh legislative assembly."

Renumber accordingly

CompTIA. The IT Industry Trade Association

Attachment 3
Page 1

January 21, 2019

The Honorable Thomas Beadle
North Dakota House of Representatives
4266 Russet Avenue South
Fargo, ND 58104-8429

Re: House Bill 1524: Relating to the Regulation of Data Brokers

Dear Representative Beadle:

I write to you today in opposition to House Bill 1524, an act seeking to regulate data brokers. CompTIA represents the country's leading technology firms, including many that are engaged in business practices with North Dakota consumers and businesses. Our members take their obligations to protect consumer information very seriously. Data is the fuel of the innovation economy and protecting consumers' information is not only a responsibility of the industry, but also a crucial business practice.

Of specific concern is the bill's sweeping and impractical requirements for businesses engaged in exchanging "brokered personal information." The new requirements set by HB 1524 impact nearly every business that uses a consumer's personal information, like a citizen's name or address, if the business does not have a direct relationship with the consumer. This sort of information is often publicly available and does not jeopardize consumers' privacy or safety. Instead, a more meaningful threshold would be the use of a consumer's personally identifiable information, which is defined in the North Dakota Century Code Chapter 51-30 – Notice of Security Breach for Personal Information.

Subjecting legitimate businesses to additional regulation by making them register as data brokers because of their use of non-sensitive information impacts the entire data ecosystem, threatening North Dakota's tech economy and the use of data-driven products and services by North Dakota residents. While the technology industry accounts for 4.3% of the overall workforce in the state, the North Dakota tech workforce earns an average of $79,8000 a year, which is $30,000 higher than the state's average private sector wages ($49,400). As local companies look to grow or out of state businesses seek to expand in North Dakota, misguided public policies like HB 1524 would factor negatively in decisions on whether to allocate resources for expansion in the state.

Despite existing statutory and regulatory protections at the state and federal level, we have concerns that additional state regulation of the industry would lead to a complex and burdensome patchwork of potentially conflicting state laws and regulations. Delivering on-demand services and content to individuals and enterprises globally – including through promising innovations such as the Internet of Things (IoT) and cloud computing – depends on access to data. Disparate requirements on a state by state level would heavily burden the data-driven ecosystem and lead to new and innovative services not being offered or provided to North Dakota consumers or businesses.

I appreciate your consideration of these points on the importance of innovation and the data economy, societal benefits of data-driven products and services, existing laws governing the industry, and the

HB 1524

CompTIA The IT Industry Trade Association

Attachment 3
Jan 21, 2019
Page 2

impact of added regulation in North Dakota. CompTIA's members fully recognize the importance of consumer trust and technological innovation recognizing they go hand in hand. As you consider the merits of HB 1524 it may be beneficial for the North Dakota legislature to study this broad topic before deciding on a legislative pathway. As only one state has passed this legislation into law, the true impact of the bill is yet to be seen.

Thank you again for taking the time to consider CompTIA's comments. Should you have any questions, please do not hesitate to contact me either via email at amadon@comptia.org or at 630.282.4332.

Sincerely,

Alexi Madon
Director, State Government Affairs – Midwest
CompTIA

CC: Representative George Keiser, Chairman, House Industry, Business & Labor Committee
Representative Glenn Bosch, Co-sponsor
Representative Corey Mock, Co-sponsor
Representative Nathan Toman, Co-sponsor

February 27, 2019

HB 1524
Senate Industry, Business and Labor Committee

Senator Klein and Members of the Senate IBL Committee,

For the record, my name is Thomas Beadle, state representative from district 27 in Fargo. I'm here this morning in support of House Bill 1524, which is now a study resolution dealing with consumer privacy protection with regards to data in North Dakota.

As introduced, this bill was a first draft on a full regulatory framework for the data brokerage industry as it impacts our North Dakota constituents. After discussion on the House side with some of the sponsors and industry players, this bill was amended into the study that you see before you.

Data privacy is a growing concern around the world, and rightfully so. Six years ago, it was said that Facebook owned the world's largest database of people that has ever been built. Since that time, they have grown from 1.2 active users to over 2.2 active users. Facebook knows quite a deal about these members. As of September 2018, Facebook could tell us publicly some simple facts:

- 1.57 billion people access Facebook daily from a cell phone;
- 1.47 billion people access Facebook daily from a desktop computer;
- 53% of users are female and 47% are male;
- 72% of l online users with an income of more than $75,000/yr are on Facebook;
- Average Facebook user has 155 "friends"; and
- Americans spend 58 minutes per day on Facebook.

Facebook is just one of many free social media tools and apps that collect data on users on a regular basis. Other popular US based companies like Twitter, Google and LinkedIn are collecting your data too. As the popular saying goes, "if you're not paying for the product, then you are the product." Software owners analyze and sell user data that is then used by advertisers. Everything from age, interests, purchasing habits, location history, health and social statistics are pieces of data that is collected, and is often collected in the background when apps are not being used.

One example of an application collecting unnecessary data is a flashlight app that turns on the LED flash of mobile phones. This simple app that only needs to control one function of the phone also has access to calendars, location and your camera. Issues like this have been brought up in court and administrative cases over the years, but often the only solution is due diligence by the end user.

There are also several cases where apps are collecting and storing information that you agree to but are not protecting or encrypting the data properly. In 2014, Starbucks was found to be storing passwords, email addresses and previous GPS information without encryption. They quickly corrected the error once it was discovered, but not all companies have been diligent in taking necessary precautions.

Currently there are no comprehensive data regulations in the United States. In 2016, the European Union passed the General Data Protections regulation with complete rollout completed in May of 2018. Without going into details, this act regulates the collection, storage and sale of data, including names, images, email addresses, social media posts, medical information, IP addresses and bank information.

This doesn't prohibit the collection of data, but requires the company to adhere to specific standards and can impose penalties on any company with an electronic presence in the European Union.

California also passed comprehensive data regulation policies in 2018 – the California Consumer Privacy Act. This act affords California residents with an array of new rights, beginning with the right to know what information companies have collected and why. It also allows consumers to request the deletion of personal information, ability to opt-out of data sharing, and access their personal information in a readily useable format.

The original bill that was introduced this session was based on legislation adopted by the state of Vermont last year and sought to define "data brokers" as companies who knowingly collect and sell consumer information to third parties, and would require them to register with the Secretary of State and develop cybersecurity procedures, while giving the Attorney General jurisdiction to enforce these requirements. The intent was to begin a much-needed conversation that will allow us to develop comprehensive data regulations and provide basic assurances to North Dakota citizens that all public and private entities operating in our state are treating the personal information they collect with the respect it deserves.

The House committee felt that it was important to study this issue and see how the hearings in Congress and in the other states play out on and wanted to make sure we had a vehicle to monitor that activity, which is why this bill is in the study form before you.

Thank you very much for your consideration on this study and I hope the committee will give it a Do Pass recommendation and keep this conversation going into the interim.

HB 1524 2/27/19 Att #2 p. 1

Gabby Reed, Manager
State Government Affairs – Rocky Mountain Region

RELX Group

Elsevier
LexisNexis Legal & Professional
LexisNexis Risk Solutions
Reed Exhibitions

February 26, 2019

The Honorable Jerry Klein
North Dakota State Capitol
600 East Boulevard
Bismarck, ND 58505-0360

Re: House Bill 1524: Relating to the Regulation of Data Brokers

Dear Chairman Klein:

I am writing on behalf of RELX and LexisNexis to respectfully request that the Senate Industry, Business and Labor Committee provide a do not pass recommendation on House Bill 1524 "Relating to the Regulation of Data Brokers". The House recently passed HB 1485 "Personal Information Disclosure Protection", which requires a much broader study of "protections, enforcement, and remedies regarding disclosure of consumers' personal data", making the well-intentioned study proposed by HB 1524 redundant.

LexisNexis is a division of RELX and is recognized as a leading provider of authoritative legal, public records, and business information which helps our customers make informed and accurate decisions. LexisNexis is the nation's leading provider of credential verification and identification services for Fortune 1000 businesses, government and law enforcement agencies, and the property and casualty insurance industry. LexisNexis plays a vital role in supporting government, law enforcement, and business customers who use our information services for important uses including: detecting and preventing identity theft and fraud, finding deadbeat parents or missing children, locating suspects, and preventing and investigating criminal and terrorist activities.

RELX/LexisNexis is supportive of the study proposed in HB 1485, which requires the legislative management to study all-encompassing privacy protections for North Dakota consumers, and looks forward to actively participating in the process during the interim. Since the study required by HB 1485 addresses all aspects of consumer data privacy, RELX/LexisNexis feels that HB 1524 would create a superfluous scope of work. Data privacy protections are critically important and deserve adequate time and study; however, it also makes sense to avoid unnecessary duplication of work and effort. Primary focus on the broad study requirements of HB 1485 would result in the most effective use of resources on this imperative topic.

Thank you for your consideration of RELX's comments on House Bill 1524. Should you have any questions, please do not hesitate to contact me either via e-mail at gabby.reed@relx.com or at 202-403-7893.

Sincerely,

Gabby Reed
Manager, State Government Affairs - Rocky Mountain Region
RELX Group

RELX Group

CC: Senator Shawn Vedaa, Vice Chairman, Senate Industry, Business & Labor Committee
Senator Randy Burckhard, Member, Senate Industry, Business & Labor Committee
Senator Curt Kreun, Member, Senate Industry, Business & Labor Committee
Senator Merrill Piepkorn, Member, Senate Industry, Business & Labor Committee
Senator Jim Roers, Member, Senate Industry, Business & Labor Committee

RELX Inc. Denver, Colorado Telephone 202.403.7893 Gabby.Reed@relx.com
www.relx.com