Dear Washingtonians:

For the past few years, I have been hearing more and more from citizens of our state that they are concerned about the protection of their privacy. They are worried about government surveillance. They are concerned about the well-publicized events in which their personal information has been exposed as a result of successful attacks against the databases of insurance companies and retailers. People, in short, feel exposed and want to know what they can do to safeguard their personal information in a world where much of that information lives on computer networks.

Washington state government has always taken privacy seriously and we make a considerable investment in securing personal data that citizens provide to over 50 state agencies, ranging from the Department of Licensing to Fish & Wildlife. Citizens provide their personal info (including their names, contact information and other personal data) to state agencies so that our state government can supply specific services, such as providing a license or other benefit. We try to do this in the most efficient and accurate manner, publishing privacy policies that are specific to each agency or state program. Nevertheless, we can do more.

Just as Washington is a technology leader in so many important fields—ranging from software development to e-commerce—we strive to set an example of “best practices” when it comes to collecting and protecting the personal information you provide while dealing with state government.
Our state agencies already have an obligation to protect your confidential information and they must exercise a high level of care to protect any records that may contain your sensitive health, financial or other personally identifiable information. In 2015, I signed a new Data Breach Law strengthening notification requirements and imposing a 45 day deadline for citizens to be notified of a breach involving more than 500 Washington residents.

While this represents a positive step for consumers, I want to make sure that our state government is taking more proactive steps to protect the private data provided to us by citizens. In April, we hired one of the first statewide chief privacy officers in the country to help develop policy around privacy law, examine new technologies that affect the privacy of citizens, and help our state government address the new issues that confront institutions in a complex digital environment.

Public education is also an important component of privacy protection. Knowing more about the use of your personal information by state government, will help you make better decisions about sharing this data. Knowing more about the way companies and social networks utilize your personal data will give you more control over your personal information. To that end, this Privacy Guide lists various resources for privacy protection sites and tools that are now available to you. We'll also publish this information on our website: http://privacy.wa.gov.

In short, I believe that informed citizens will make the best choices about their personal data and that our government needs to be open and transparent in this regard. That’s why we are publishing this Privacy Guide and creating new initiatives to protect the personal data that we hold in trust for you.

Sincerely,

Jay Inslee

Gov. Jay Inslee
INTRODUCTION FROM WASHINGTON’S CHIEF PRIVACY OFFICER

This Privacy Guide is the first of its kind for the state of Washington. When you engage with state government, it’s likely that you provide personal information to a state agency or program in order to get a product or service, such as a driver’s license or health care benefit. Increasingly, people transact their business with the state via the Internet and entrust the security of their personal information to us. Like all modern institutions, we operate in a climate of digital information, data centers and cloud services. And practically every day we read headlines about cyber-attacks and the threat to personal privacy online.

When I was hired earlier this year to serve as the state’s chief privacy officer, I quickly determined that we do a good job describing the kind of information we collect and telling people how it is used. Each state agency publishes its own privacy policy and we also have a “portal” site called Access Washington (http://access.wa.gov) that provides a broad overview of our government services, indexed by topic.

However, we can do a better job informing you, as consumers of our services, of how to protect your personal information in an increasingly challenging online environment. You can apply the tools and articles referenced in this Privacy Guide to your activity on commercial websites, social networks and other sites that you access, whether on your personal computer or a mobile device. We believe that the best informed citizens will want to control their personal data and not expose themselves to data sharing and other practices that they do not intend to authorize. We also want to share what we know about “best practices” for safeguarding your information in the digital world.

Alex Alben, Chief Privacy Officer

This guide provides four kinds of information:

- A description of the types of information collected by Washington state agencies
- Privacy tips and charts describing top threats to personal data
- Privacy and security protection tools
- Explanations of Washington’s Public Records Act and open data initiative

The online version of this guide can be found at: http://privacy.wa.gov. We intend to update this site frequently with current articles and other useful resources about privacy protection.

We hope that this guide and the accompanying online materials give you a fuller sense of both your privacy rights and our commitment to ensuring that state government does everything in its power to safeguard your personal information.
In order to protect your privacy, you may wish to use a variety of tools produced by private companies. When choosing privately made tools, it is safest to rely on established companies and research reviews from reputable websites. While the state of Washington does not endorse any such tools, the list below contains some that web users have found convenient, useful, and safe. In each case, alternate applications are available from other software makers, and you should choose the ones that best meet your needs. Type the bold phrases into any search engine to find a link to the tool you are looking for.

**Microsoft Security Essentials**
scans the programs you run to determine whether they contain malware, disposing of any that prove to be dangerous. It also scans your system to make sure no infections have gotten through. It’s both free and easy to use.

**Anonymizer**
is a tool that encrypts and anonymizes Internet traffic.

**Spybot Search & Destroy**
eliminates spyware by scanning your computer and eliminating dangerous files.

**Password Maker**
is one of many online password safes, which save you the trouble of remembering numerous different passwords. You create a single, master password, and it creates strong, secure passwords for all the different sites you use. MyDLP (data leakage protection) identifies sensitive data and prevents data from leaking via the Web, email, removable devices, printers and other channels. In addition to the free community version, it also comes in a paid enterprise version that includes support and some additional features.

**Ad Bloc Plus**
is an add-on available for Mozilla and Chrome browsers. It blocks pop-up advertisements and associated tracking cookies.

**Digital Advertising Alliance**
has an opt-out tool for “interest based” advertising which allows you to choose which ads you want to exclude from your system.

**HTTPS Everywhere**
is designed to protect your privacy when you visit specific sites, including Facebook, Google Search, the New York Times, PayPal, Twitter, The Washington Post, and Wikipedia. Note that it protects you only on sites that employ the HTTPS secure protocol. It can't protect you when you use other Internet services such as instant messaging and client-based email.
THE PRIVACY AND SECURITY LANDSCAPE

Every day brings new headlines warning us of data breaches and major “hacks” of networks that contain secure data, often including sensitive personal information. In the past year, the breaches at Target, Premera and the federal government’s Office of Personal Management raised major issues about the methods both private companies and governmental organizations are using to secure data in a climate of cyber-attacks, often launched by well-educated and well-funded hackers operating overseas.

Some security experts warn that “assumption of breach” has become the new normal, where every data network will be compromised at some point. Citizens increasingly worry about the security of personal information they entrust to online entities. Yet, given the fact that so much of our interactions have moved online, consumers often have little choice but to “trust” a company or agency with their personal information.

With privacy as our core value, society should make the appropriate investment to secure and respect the personal information of private citizens.

Security is not an end in and of itself. In an economy where governments and corporations spend billions of dollars for network security, we should reflect and consider the values we are truly trying to safeguard—namely the personal privacy of individuals to conduct their lives without intrusion or unwanted exposure.

At the state government level, we’re keenly aware of our obligation to safeguard the information the citizens of Washington provide to us in order to avail themselves of state services. We’re also aware that we continue to operate in an atmosphere of cyber-attack, where hackers try to penetrate and compromise our networks and data centers.
NEW STRATEGIES

New environments often require new strategies and we strive to meet the challenges posed by cyber-attacks in the digital age. To this end, we have begun to develop new strategies to maximize privacy protection across state government:

**Data Minimization**—a highly effective way to reduce the risk of data breach and any damage caused by breach is to collect only a minimal amount of data from citizens and to retain that data only as long as necessary to render a particular service.

**Transparency**—consumers need to make informed choices about the types of information they share online and state agencies must fully disclose their data sharing practices and be available to explain our policies and procedures relating to privacy.

**Public Education**—we want to provide the citizens of Washington with the tools and information they need to maximize their privacy protection. This Privacy Guide is an initial attempt to begin that education process.

Making the proper investments in both privacy and security is a work in progress as new challenges arise and new technologies are deployed across digital devices and networks. We welcome your thoughts on how to make these investments in the service of our core values, such as privacy. Visit us at http://privacy.wa.gov.
TOP 10 PRIVACY PROTECTION TIPS

1. Always read websites’ privacy policies before handing over personal information. Understanding when and how your information may be shared will allow you to decide whether or not to do business with certain companies. If a company does not post a privacy policy, be very wary; it may be advisable to contact such companies and ask their policies before sharing any of your personal information.

2. Never share personal or financial information such as social security or credit card numbers through non-secure sources like email, text messages, and social media postings. Identity thieves often disguise themselves as representatives of trusted companies and ask for your personal information. Legitimate companies rarely ask you to share personal information over email.

3. Educate your family about the risks of sharing personal information online. If your children have access to credit cards or bank accounts, make sure they understand the risks of sharing that information with anyone, even their friends. Encourage your children to check with you before sharing any sensitive information.

4. Create secure passwords. It is best to have different passwords for each website that has access to your personal information, so that if one site has a data breach hackers will not be able to use your password to access your records in other sites. Never use simple personal information such as family or pet names, birthdays, or home towns in passwords; avoid using any information about yourself that is available online to create your passwords. Even password reminders should not contain personal information.

5. Make sure your home network or wireless system has password protection, anti-virus software and a firewall.

6. Never download email attachments or web apps unless you are sure of their origin and legitimacy. Hackers use attachments and apps to infect your computer with viruses, worms or spyware that can damage your computer or expose your data to online intruders. If friends or contacts have viruses on their computers, they may unknowingly forward those viruses to you through email; even if an attachment is from a friend, don’t download it unless you are sure of its contents.
TOP 10 PRIVACY PROTECTION TIPS

7. Lock or log off from your computer whenever you are not using it. Do not leave it unattended in a public location. Even if you are just stepping away for a moment to get coffee, be vigilant; it only takes a minute to compromise your data.

8. Regularly check your credit reports and statements to make sure your financial information has not been compromised. You are legally entitled to a free annual credit report at http://annualcreditreport.com.

9. Use your web browser settings to manually control cookies on your computer. Cookies are information tidbits that websites store on your computer to speed up web browsing by automating things like passwords and URLs. But they can also be used to compromise your computer security. Make sure you only accept cookies from sites you trust.

10. Remember email is forever. Always consider the consequences of email being forwarded to unintended recipients.

What are the Most Common Methods of Access?

- Traditional Methods
  - Lost or stolen wallets, 43%
  - While conducting a transaction, 19%
  - Stolen paper mail, 3%
  - “Friendly” theft, 13%
  - Online, 11%
  - Data breach, 11%
  - Other, 1%

Source: Javelin Strategy & Research
WHAT THE STATE OF WASHINGTON COLLECTS/KNOWS ABOUT YOU

What type of information does the state of Washington collect when you visit a website or provide us with data to get a specific service? In general, when you visit a state agency website or a portal site such as Access Washington (http://access.wa.gov), non-identifying information is automatically collected. This information includes your IP address and the domain name of your internet service provider; the type of browser and operating system you use; and the pages or services you accessed at the site. This information is used to improve the content and services of the state’s websites.

There are times when you’ll be asked to provide personal information at a state site, including when you participate in a survey or perform some transaction online. Providing this information online is always voluntary. It may include your email address and the contents of email you send to the state, or information used in online transactions, and will be stored in accordance with Chapter 40.14 RCW, Preservation and Destruction of Public Records.

We use this information to perform services, respond to questions, and address issues you may identify, including suggestions to improve our website. We may also forward your email to another agency for appropriate action.

The state attempts to minimize the amount of data gathered whenever possible and collect what is deemed necessary and appropriate.

http://access.wa.gov
STATE GOVERNMENT AND OPEN DATA

State data is like any other asset of state government - it belongs to the citizens. Some of that data is specific to a person, and needs to be protected rather than shared. But a lot of the data collected by state agencies is not private - it's public and publishable. Fish counts in the rivers; traffic on the roads; tax dollars spent on government; the population of a county -- these are all bits of data that the state collects and uses to keep key services and resources running smoothly. But much of this state data has a secondary use outside government that may be just as important to citizens: population data is also useful to scholars tracking economic development; traffic data can help people get home safer; fish data helps salmon stay off the endangered species list; and government spending data helps local companies win state contracts.

Since 1996 state agencies have been encouraged to make information available electronically where appropriate. Since 2010 it's been called "open data" and the state has supported a variety of common web portals for agencies that make it easier to publish data in a way that computers, newsletters and browsers can easily use. For example - http://data.wa.gov presents tabular data on a wide variety of topics; http://geography.wa.gov lets citizens explore state mapping data; http://fiscal.wa.gov shows where the public's money goes. Most agencies have their own "reports and data" section on their website. Cities and counties are also important contributors to open data - Seattle, Redmond, Spokane, and Tacoma each have their own open data sites. So do Pierce and King counties.

Here's a fairly complete census of local open data sites: http://us-city.census.okfn.org. We've been doing this for a number of years, and the availability of this data from the state has made a difference to a number of companies, nonprofits and researchers - helped them pivot to a new line of business, find the right place to expand operations, or understand government projects.

Though you won't find your personal data on state or city websites, you may be able to find government data that helps you accomplish your personal and professional goals. Think flexibly and take a look.
PRIVACY AND WASHINGTON STATE PUBLIC DISCLOSURE LAWS

Washington state believes in sunshine! In 1972, the citizens of our state voted for Initiative 276, creating one of the most extensive public disclosure laws in the country, ushering in an era of transparent government and allowing citizens to request public records relating to the operation of government agencies, political campaigns, lobbyists and public spending. These statutes, known as the Public Records Act, have been revised quite often over the past 40 plus years. If you want to look up specific information about the act, do a search for “42.56 RCW.”

Most activity by state government is covered by the Public Records Act. The law applies to governments at all levels in our state, including cities, towns, counties and special purpose districts. Our Public Records act does not apply to the judicial branch of government. State legislative records are covered by the act. For a full list of public disclosure resources available to you, visit http://pdc.wa.gov.

The definition of what constitutes a “public record” under the law is quite broad. For example, emails, text messages, photographs, video files, audio files as well as written records and correspondence all fall under the definition. (See 42.56.10 for the complete definition.)

The law recognizes that there may be cases where the disclosure of a particular public record might be “highly offensive” to a reasonable person and therefore does not mandate disclosure if such a record is not “of legitimate concern to the public.” Otherwise, there is no privacy right under the Public Records Act.

In general, Washington enjoys the benefits of a robust Public Records Act and both local and state governments dedicate personnel to handling public records disclosure requests.
PERSONAL PRIVACY EXEMPTIONS TO PUBLIC DISCLOSURE LAWS

Personal information may be included and disclosed under the Public Records Act. However, there are eight specific exemptions for the following categories of personal information. Here is an edited excerpt from the statute listing the eight exemptions:

1. Personal information maintained for students in public schools, patients or clients of public institutions or public health agencies, or welfare recipients.

2. Personal information of a child enrolled in licensed child care in any files maintained by the Department of Early Learning; or for a child enrolled in a public or nonprofit program serving or pertaining to children, adolescents, or students.

3. Personal information in files maintained for employees, appointees, or elected officials of any public agency.

4. Information required of any taxpayer in connection with the assessment or collection of any tax if the disclosure of the information to other persons would: (a) Be prohibited to such persons by Revised Code of Washington (RCW); or (b) Violate the taxpayer’s right to privacy or result in unfair competitive disadvantage to the taxpayer.

5. Credit card numbers, debit card numbers, electronic check numbers, card expiration dates, or bank or other financial account numbers, except when disclosure is expressly required by or governed by other law.

6. Personal and financial information related to a small loan or any system of authorizing a small loan in RCW.

7. Any record used to prove identity, age, residential address, social security number, or other personal information required to apply for a driver’s license or identification card.

8. All information related to individual claims resolution structured settlement agreements submitted to the board of industrial insurance appeals under RCW 51.04.063, other than final orders from the Board of Industrial Insurance Appeals.

In 2015, the Legislature expanded the definition of exempt “personal information,” adding “financial information” as defined for purposes of identity theft crimes, including social security numbers. You can find the full provisions of the law at RCW 42.56.230.
Privacy has emerged as a leading topic in a technology industry that has traditionally been focused on systems, services and security. Those of us who manage information technology or “IT” organizations have come to realize that data lies at the heart of what we wish to protect. This is especially true for state government, where our agencies collect many types of data from citizens who need to receive services from the state.

The importance of privacy in the digital age cannot be underestimated. In fact, many of us believe that privacy represents the new frontier of human rights. Without privacy, what freedom does an individual have in our society?

My agency—Washington Technology Solutions—is responsible for crafting security and technology policy for our state. While our state agencies and programs already had articulated privacy policies for the treatment of citizens’ personally identifiable information, we thought it was important to go further and more deeply embed privacy into the way we do business in our agency. As a result, we recently instituted the following new initiatives designed to promote both privacy and security:

- Created the State Office of Cyber Security.

- At the request of the governor, leading a commission to study new drone technology and examine the issues relating to the deployment of drones by state agencies.

- Creating a privacy work group among state agencies.

- Hiring the country’s third chief privacy officer to coordinate and lead new programs relating to privacy on a state wide basis.
We know we must continue to adapt to a rapidly changing environment, which includes both new technologies and new types of attacks from hackers who wish to compromise the user data we collect and retain. To accomplish this, my office has put a premium on hiring talented people with experience in a broad range of industries. In addition, we embrace new methods and techniques for developing software and for organizing our service teams. We realize that in order to succeed in our mission to position Washington for the future, Washington Technology Solutions must attract individuals who bring diverse skill sets to solve complex problems.

We aim to promote best practices relating to both privacy and security for our state. We hope that this Privacy Guide and the associated website http://privacy.wa.gov represent a significant first step toward educating people in our state about our privacy policies and the ways that consumers can protect their privacy online.

Sincerely,

Michael Cockrill
CIO, Director of Washington Technology Solutions

ABOUT WATECH

Washington Technology Solutions (WaTech) is “the consolidated technology services agency” (RCW 43.105.006) charged with enabling public agencies to better serve the people of Washington State via technology. WaTech operates the state’s core technology infrastructure—the central network and data center; supports enterprise applications; and, innovates services and practices through e-Government. The agency is also charged with preparing and leading the implementation of a strategic direction and enterprise architecture for state government IT. Additionally, WaTech houses the state’s chief privacy officer, the State Office of Cyber Security, and Washington OneNet.