Internet Privacy Practices Self-Assessment		
This assessment is used to calculate an Internet privacy practices score. This is not a test; this is a tool to help you understand your privacy practices. Take notes and write in the margins - use this rubric as a guideline to inform your assessment and feel free to adapt and make changes where you see fit. Add your total for each category, then use your grand total to find your range. The results are intended to inform your Internet privacy decision making and any changes made cannot guarantee privacy.		
Practice/Download/Configuration	"+/- points"	Your score
Operating System: Perform this entire assessment for one machine at a time, beginning with the operating system you most commonly use		
Windows	1	
OSX	2	
GNU/Linux	3	
Tails	4	
Other:		
Total for Operating System		
Internet Browser: Complete a different assessment of each browser, and begin with the browser you use most often		
Internet Explorer	0	
Safari	0	
Chrome	1	
Firefox	2	
Tor	3	
Other:		
Total for Internet Browser		
Browser Add Ons and Extensions: Add points for the add ons that are currently installed on the browser you are assessing		
HTTPS Everywhere!	1	
Privacy Badger	1	
AdBlock (Potentially compromised)	0	
uBlock Origin	1	
Disconnect.me	1	
AVG Do not Track	2	
Total for Browser Add Ons and Extensions		
Browser Configurations and Practices: The specific terms may differ in each browser. As always, use your best judgement		
Send a "Do Not Track" request with your browsing traffic	1	
Block third party cookies	1	
Block sites from setting any cookies	2	
Delete cookies after closing browser	1	
Do not automatically run plugin content	2	
Do not allow any sites to show pop-ups	1	
Do not allow any site to track your physical location	1	
Manually delete browser history and cookies every 1-4 weeks	3	
Manually delete browser history and cookies once every 6 months	2	
Manually delete browser history and cookies once every year	1	
I have never deleted my browser history and cookies	-1	
Add 1 point for each additional intentionally set privacy configuration		
Total for Browser Configurations and Practices		
Passwords: If you have many online accounts, focus on the ones most important to your privacy (for example: email, social media, and banking)		
You reuse passwords for multiple accounts	-2	
Your passwords are very weak (password123)	-2	
Your passwords are medium (more than 11 random characters, symbols, and numbers	2	
You use passphrases (5+ random words (ex. CorrectHorseBatteryStapleCanoe) from the Diceware list)	3	
You use an encrypted password manager (ex. Dashlane, KeePass, KeePassX, etc.)	3	
You use a non encrypted password manager (excel, word document, post its, notebook)	-2	
You store your passwords in your browser	-2	
You do not have a passcode on your cell phone	-1	
You have a four digit passcode on your cell phone	1	
You have a passcode on your cell phone that is longer than 4 digits	2	
Total for passwords		
Social media: Add or subtract points based on your social media practices		
No social media accounts (Facebook, Twitter, Instagram, Tumblr, etc.)	3	
Full name not listed on social media accounts	2	
Profile is fully private	1	
You review your privacy settings at least once every six months	1	
You use two factor authorization for your social media log-ins	2	
Total for Social Media		
Email: Consider doing different assessments if you have multiple accounts		
You use two factor authentication to log in to your email	4	
You use a free email service (Yahoo or Gmail)	-4	
You download files or click on links sent from unknown sources	-5	
Your sensitive emails are encrypted	4	
All of your emails are encrypted	8	
Total for Email		
Apps: Mobile applications you can install on your devices to run special programs. Security varies significantly		
You research an app's credibility before downloading	4	
You are selective in the permission you grant apps (limited access to photos, other apps, location services, etc.)	5	
You store sensitive information in apps that are not encrypted	-4	
Total for Apps		
Encryption: Encryption scrambles your data so no one can access it without your special password		
Your text messages are encrypted using Signal	3	
Your phone calls are encrypted using Signal	4	
Your hard drive is encrypted	4	
The data on your cell phone is encrypted	4	
Total for Encryption		

Advanced Privacy Practices		
You use throw away emails for unimportant online accounts	5	
You receive Haveibeenpwned updates for your accounts	5	
You do not use public wifi	5	
You use a VPN to use public wifi	5	
You use the Tor browser for private browsing	5	
You have logged in to a personal email, social media, or banking account on Tor	-1	
You use Tails for anonymous and amnesic private browsing	10	
Total for Advanced Privacy Practices		

Totals From All Categories	
Total for Operating System	
Total for Internet Browser	
Total for Browser Add Ons and Extensions	
Total for Browser Configurations and Practices	
Total for passwords	
Total for Social Media	
Total for Email	
Total for Apps	
Total for Encryption	
Total for Advanced Privacy Practices	
Grand total	

Grand Total Range	Summary	Recommendations
0-25	You probably haven't done much configuring to your browser or operating system in order to better protect your privacy. The good news is that there are a lot of ways you can begin protecting your Internet privacy! See the recommendations section for a few things you can do right now to improve your Internet privacy, and try incorporating a few of the new concepts into your regular practices.	1. Delete your browser cookies and history 2. Add the extension "Privacy Badger" to your browser 3. Add the extension "HTTPS Everywhere!" to your browser 4. As you log into your accounts, change your passwords 5. The best thing you can do is educate yourself - go to the sources listed below to learn more about Internet privacy
26-50	You have some of your settings already configured to better protect your privacy - good job! See the recommendations at right for a few things you can do to get your Internet privacy protection to the next level. You can also look back through the assessment for low scoring categories to improve - consider learning more about and implementing the specific practices you don't already employ.	1. Configure your browser to automatically delete your data when you close it 2. Add an extension to your browser that blocks trackers 3. Enable two factor authentication for your most important accounts 4. As you log into your accounts, change your passwords to passphrases 5. The best thing you can do is educate yourself - go to the sources listed below to learn more about Internet privacy
51+	You are on the right track! You have done a considerable amount of work to ensure your Internet privacy. While privacy and anonymity can never be guaranteed, you are following the best practices as of print. Stay educated and make sure you share the importance of Internet privacy with your friends, family, and coworkers. Consider getting involved with an organization that creates or influences Internet privacy policy.	1. Encrypt your common methods of communication (phone, email, etc.) 2. Consider using the Tor browser for sensitive browsing 3. If possible, invest in a good password manager 4. Start using fake email accounts to sign up for unimportant online services 5. The best thing you can do is educate yourself - go to the sources listed below to learn more about Internet privacy

To learn more, visit the following sources:

The Tor Project	https://www.torproject.org
Electronic Frontier Foundation	https://www.eff.org
The Library Freedom Project	https://libraryfreedomproject.org
The DIY Guide to Feminist Cybersecurity	https://tech.safehubcollective.org/cybersecurity