Privacy in a Synchronized World

Do you know where your data is?

WHITE PAPER

Author
Stan Kiefer
Senior Security Researcher, Cyber Security Services, Symantec
Contents

Taking Stock of Our Digital Exhaust ........................................... 03
  The Scary Secret Behind the Synchronized World ..................... 03
  Looking Under the Covers of Synchronized Services ............... 03
  Synchronization is Purpose-Built for User Convenience .......... 04
Apple iCloud ............................................................................ 04
  The Risk ............................................................................... 04
  The Implications .................................................................. 04
  Privacy Violations ................................................................ 04
  Data Leakage ....................................................................... 04
  Data Exfiltration .................................................................. 05
  Mitigation ............................................................................ 05
  iCloud Experiment—Can iMessage Data be Encrypted at Rest? . 05
  The Experiment ..................................................................... 05
  The Extension ....................................................................... 05
  Results .................................................................................. 05
  Practical Tips ........................................................................ 06
Google Chrome ........................................................................ 06
  The Risk ............................................................................... 06
  The Implications .................................................................. 07
  Mitigation ............................................................................ 07
  Potential Actions to Take—Practical Tips ............................. 07
Conclusion ............................................................................... 08
About Cyber Security Services ............................................... 08
Take the Next Steps ................................................................. 08
Taking Stock of Our Digital Exhaust

We leave traces of ourselves everywhere we go. We provide bits and pieces of information to every person, place, and organization we interact with on a daily basis. In the physical world, these bits and pieces tend to remain isolated: The barista knows your name and coffee order, the maître de knows your favorite booth, the grocery store knows your ice cream choices, but that’s about it. They are not syncing and storing all your orders, preferences, searches, contacts, travel, or meetings for use at some later date. But in the online world, it’s a different story.

Online, all the bits and pieces of information you reveal about yourself as you go about your daily activities follow you around. They are your digital exhaust, so to speak, and it’s important to be mindful of all the traces you could be leaving behind as you roam. Unfortunately, this is easier said than done in today’s highly connected and synchronized world.

Your data exhaust trail is probably a lot more extensive than you may think. There is all the information you post, share, and store in your online public profiles, but there is also a lot of other information that’s tracked, transmitted, and stored about you by all the different devices, networks, and services you use. Your data is synced, siphoned, and collected in the background, often without your explicit knowledge: Apps on your smartphone likely send location data on you right now; your smart TV shares your viewing preferences based on what you just watched; and retailers refine advertisements and offerings based on what they just learned about your buying preferences and patterns.

Even apps you don’t use may collect information on you. Recent reports revealed that apps were sending sensitive information to Facebook even on people who didn’t have a Facebook account. There are also data trails that other people inadvertently leave about you when they tag you or upload your contact information to a service, for example. Your synchronized services compound the problem, all in the name of convenience.

The Scary Secret Behind the Synchronized World

Application and operating system synchronization services are designed to make your life easier. They replicate your personal data and preferences between devices, networks, and services, so it follows you wherever you go, whenever you need it. These services allow you to pick up exactly where you left off, whether you are on your phone, TV, tablet, or computer; they save you from laboriously entering the same thing multiple times; and they enable everything to run smoothly, all without your input. These services, however, bring unintended consequences that raise privacy concerns, on both a personal and business level.

 Often, the data storage systems used by these services do not encrypt your data at rest, leaving it vulnerable, in plain text, to tampering, theft, or analysis by the companies collecting it. Sometimes these services make the synchronized data accessible to third-party applications or networks without your knowledge. Other times, when they are used on borrowed, shared, or public devices, they leave remnants of your personal information behind.

Looking Under the Covers of Synchronized Services

The Cyber Security Services research team at Symantec decided to take a deep dive into the world of synchronized services to uncover low level details around the way the services function and what data is involved in each service. The end goal was to uncover what, if anything, could be done to identify any potential privacy concerns associated with the services and the related data.

We looked at two of the top synchronized services—Apple iCloud® and Google Chrome®—to understand what information is at stake with these services of convenience and to analyze the implications of transport and storage of the data involved from both an individual and business perspective. We also identified steps to lower the potential privacy risk and highlight areas of concern. The following is what we found.

---

Synchronization is Purpose-Built for User Convenience

It’s important to clarify that the two synchronization services our research team analyzed were purpose-built for convenience, to help users effortlessly move across devices and services without having to think about their data. At no time during our research did we find any security vulnerabilities or other issues with the identified services; each functioned as advertised and documented.

Apple iCloud

iCloud is Apple’s central cloud storage and account management system. It is “built into every Apple device. That means all your stuff—photos, files, notes and more—is safe, up to date, and available wherever you are. And it works automatically, so all you have to do is keep doing what you love.”

iCloud syncs information across devices and services

<table>
<thead>
<tr>
<th>Devices</th>
<th>Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>iPhone®</td>
<td>iCloud Drive</td>
</tr>
<tr>
<td></td>
<td>Backup</td>
</tr>
<tr>
<td>iPad®</td>
<td>Mail</td>
</tr>
<tr>
<td></td>
<td>Photos</td>
</tr>
<tr>
<td>iPod®</td>
<td>Messages</td>
</tr>
<tr>
<td></td>
<td>Notes</td>
</tr>
<tr>
<td>Mac®</td>
<td>Keychain</td>
</tr>
<tr>
<td></td>
<td>Reminders</td>
</tr>
<tr>
<td>Apple TV</td>
<td>iWork</td>
</tr>
<tr>
<td></td>
<td>Siri</td>
</tr>
<tr>
<td>Windows® PC</td>
<td>Calendars</td>
</tr>
<tr>
<td></td>
<td>Safari including bookmarks, autofill, and passwords</td>
</tr>
</tbody>
</table>

The Apple default setting shares information across all devices, so that you have access to the data associated with these apps, no matter what device you are using. Other third-party apps also use the iCloud drive to store, share, and synchronize data across devices.

The Risk

Other than Apple Backups, the data stored on Apple devices is typically stored in plain text databases (SQLite DBs) or in proprietary flat file formats with binary metadata. This renders your information vulnerable to theft if the device is compromised or synchronized and stored in a place you did not intend it to be. That’s a lot of information: Think of all your messages, notes, photos, documents, passwords, and the like.

The Implications

What does this data exposure potentially mean for you, as an individual and as a business? We looked at a few scenarios to better understand the following:

Privacy Violations

If you use the same iCloud account across your personal and corporate devices, you trigger a host of unintended consequences. All the information in apps, such as iMessage and Notes, are replicated and stored in clear text on both your personal and corporate systems. Safari data is also shared between all Apple devices, so your history, bookmarks, passwords, and autofill, which includes all your contacts and any data you once typed in a web form, are also stored in clear text on all your systems.

If your employer regularly scans your devices, you share a whole host of personal information with them that you may or may not have wanted to share, from photos and texts to browser search history and passwords. Now, without intending to, and without actually doing anything from your corporate machines, on corporate time, you may find yourself having to answer questions you weren’t prepared to discuss with your employer. Worse yet, you may find yourself in violation of your company’s acceptable use policies—simply because of the replicated data now stored on those corporate machines, behind the scenes, without your interaction.

Data Leakage

If you don’t keep personal and corporate accounts and devices completely separate—NEVER using one to access the other—it is likely any corporate data synchronized to iCloud is also replicated to your personal Apple devices. This means that documents you created in the native Notes application on your company Mac that contains sensitive or regulated information are also stored on your Mac at home or your personal iPhone, if you ever use that corporate account on your personal device.

5 https://www.apple.com/icloud
In most cases, your personal networks are easier for hackers to compromise than your company’s networks. Once your personal machine is compromised, the attacker has access to all the synchronized corporate data on your device. This attack vector is now prevalent: as corporate defense systems become stronger, attackers increasingly target employees at home in the hopes of finding valuable information outside of corporate strongholds. The default from Apple is to share information across all devices, so that you have access to the data associated with these apps no matter what device you are using. Other third-party apps can also use the iCloud drive to store and share data and have it synchronized across devices.

Data Exfiltration

For a malicious insider, iCloud synchronization could be the perfect tool for bypassing many forms of data loss prevention (DLP) and other security measures to exfiltrate valuable data and company secrets. For example, an employee stores exfiltrated data in Notes or iMessage as an attachment, then simply retrieves the data from a personal device, outside of corporate controls.

Mitigation

We looked at whether it was possible to limit personal data exposure while maintaining the benefits of the iCloud synchronization services. The simple answer, based on our experimentation, is no. Apple tightly controls the way its services and devices are used. Its proprietary way of managing its native applications, and how it stores the data, means once you try to make any changes, the applications often become corrupted and simply stop working as designed.

iCloud Experiment—Can iMessage Data be Encrypted at Rest?

We wanted to see if we could store iMessages encrypted at rest (using a user-supplied passphrase) so they couldn’t be easily read or intercepted while stored locally on MacOS computers. Currently, the chat.db stores clear text messages in an SQLite format. We experimented with adding an extension to the iMessage app so it would store all conversations encrypted in the chat.db. Here is what we did:

The Experiment

We experimented on MacOS 10.14.x and 10.13.x, setting a different location each time for the chat.db file. Modifying the chat.db file did not immediately impact the conversation within the Messages app. Rebooting, after modifying a conversation text within the chat.db file, caused all conversations within the Messages app to disappear, even though they persisted within the chat.db file itself.

Figure 1. chat.db table in SQLite DB format

The Extension

XCode via Swift lets you add an iMessage extension to any app—game makers use this extension to enable users to play games within iMessage and create stickers. We postulated it would be possible to use an in-app encryption extension. Doing so requires each person within the conversation to use decryption phrases or keys to communicate with each other person, and to store those keys in a separate location outside the Messages application. After several team discussions, we decided this was too cumbersome; most users would not go through the extra effort to add the at-rest privacy.

Results

After performing several additional tests, we determined that modifying the chat.db directly is a non-starter: Encrypting conversations stored on disk isn’t easily achievable, if possible at all. The same holds true for the Notes app. As a result, we conclude that, until Apple decides to encrypt the data within the files on disk, using these services raises potential privacy concerns. During our testing, we found:

6 https://developer.apple.com/documentation/messages/icecreambuilder_building_an_imessage_extension
1. **Modifying the chat.db corrupts the data.** When we tried to encrypt the information, all messages in the app were truncated to the last message received or sent. It turns out there is a checksum related to the message text, so modifying the message without changing the checksum corrupts the data. This means any solution other than an Apple API modification won’t work.

2. **Modifying an archived message does not improve the security of the data.** The modifications did not affect the conversations that appear within the Messages app when it starts, even when the device is restarted.

3. **It is difficult to restore data that has been corrupted.** Restoring backups of the iMessages folder did not restore conversations. Only messages synced by iCloud were eventually restored, but only after we restarted the device. Sometimes we had to restart the device multiple times to restore the conversations to a noncorrupted state.

It appears that only Apple, not a third party, is possibly able to safeguard at-rest data. Even if we could conceive of a way to encrypt the data at rest, the differences in how data is stored between different operating system versions, plus the differences between how data is stored on different iOS devices, makes managing a holistic solution extremely difficult.

**Practical Tips**

Short of not using these services, there are a few things you can do to minimize the potential risks.

- **Keep personal and business iCloud accounts completely separate**—never access business accounts on personal devices and vice versa—to prevent inadvertent data leakage.
- **Disable the iCloud drive** to prevent data from leaving the corporate network through this channel. It is important to recognize this will limit exposure, but other apps may provide exfiltration paths used by an insider threat.
- **Turn off autofill within Safari.**
- **Use your iCloud account only on trusted resources;** never use it on shared public systems or borrowed devices that you cannot factory reset after use.
- **Ensure your clipboard is empty before you transition to another device** (desktop to mobile), especially if passwords or other sensitive data are left in the clipboard.

### Google Chrome

Chrome login, via Google accounts, provides a number of built-in synchronization services for seamlessly transitioning from one device or network to another. Chrome synchronizes the following by default:

- Apps
- Bookmarks
- Browsing History
- Open Tabs (pass the tab)
- Themes/Wallpaper (browser-based, unless using Chrome books)

Users are able, however, to elect whether or not they want to sync individual apps and data within the applications themselves.

**The Risk**

There can be serious privacy issues with Chrome data storage and synchronization, from both a personal and corporate perspective. Google stores most data in clear text by default, so we found many of the same issues—regarding privacy, data leakage, and data exfiltration—we outlined for iCloud’s synchronization.

If you use your personal Google account to sign into Chrome on your corporate system, your personal data will follow you;
if you sign into your corporate account from your personal system, corporate data will be stored on those personal devices.

One difference between the Google and Apple services: Synced data is available to Google without your password and it is stored, in clear text, within the Google infrastructure itself. To protect your data within the Google infrastructure, you must create a passphrase to encrypt the data, and then provide this passphrase each time you open the Chrome app on any device.

The Implications

Google is able to access all the personal and corporate information that’s been synced, scan it, and use it for their own purposes. It is also possible they provide access to third parties. Think of the ramifications of Google (or a third party) scanning the browser history for your entire company and mining it for data. Imagine a competitor’s advantage if they gain access to ‘anonymized’ versions of your company’s browsing data. Not to fuel unfounded conspiracy theories, but we do not discount that data collection and mining is a major part of Google’s business.

Mitigation

Given the many similarities between the Apple and Google implementations, we didn’t conduct any Chrome experiments because we believed the outcomes would be the same – it would not be possible to add measures to encrypt data at rest. Instead, we focused on documenting the steps individuals and businesses could take to try to mitigate the risks to their data.

Potential Actions to Take—Practical Tips

To better protect the integrity and privacy of your data:

- **Get a summary of data held in your Google account.** You can then decide which synchronization and data collection services you wish to turn off.
- **Use incognito mode.** Select “File” then select “New Incognito Window” to ensure your browsing history is not stored locally. Note that Incognito mode does not provide anonymous browsing; you are still tracked by websites, and data stored in memory and deleted files on your hard disk are still recoverable using forensic techniques.

  - **Turn off synchronization capabilities** on devices that you do not wish to store data on or share data from.
  - **Do not use your personal Google (Gmail) account** on your work computers.
  - **Secure sync data via a passphrase to encrypt it at rest;** otherwise, Google stores it in clear text. According to Google, all synchronized data may be encrypted, rendering it unreadable by Google.
  - **Turn off the auto form fill feature** within Chrome.

Conclusion

We billow personal exhaust as we motor around the digital world. We carry tracking devices in our pockets, are surveilled by our televisions, and use apps that siphon data from us all the time. Once our data is out there, it can be used, or misused, in ways we never anticipated. It is important we get a handle on our information and make conscious decisions about what is out there, so we can exert some control over how it is used.

We are not suggesting that applications and operating systems collect our data without informing us; we all see the license agreements and usage policies tied to all the services we so heavily rely on today. But, most of us click ‘yes’ or ‘agree’ before we even read the first sentence. In the end, if we know the price we pay for all this convenience, does it change what we do?

As we move ahead in this digitally connected world, we need greater awareness of the real cost of using all these devices and applications. Now is the time to evaluate what we are potentially giving up before we turn our personal information into the currency of a surveillance economy.

---


4 [https://support.google.com/accounts/answer/162744?hl=en](https://support.google.com/accounts/answer/162744?hl=en)
About Cyber Security Services

Symantec™ Cyber Security Services bolsters your in-house security program with an integrated services portfolio no other vendor can match—powered by Symantec global threat intelligence, advanced analytics, machine learning, and the unequalled human expertise of our cyber security warrior network.

Take the Next Steps

Accurately predict, quickly detect, and effectively respond to threats and attacks. To learn more about—Cyber Security Services—please visit go.symantec.com/CSS

DeepSight Intelligence—please visit go.symantec.com/DeepSight

Managed Security Services—please visit go.symantec.com/MSS

Incident Response Services—please visit go.symantec.com/IncidentResponse

If you are experiencing an incident, contact the Incident Response Services team directly.

Email: incidentresponse@symantec.com

Phone:
United States: +1 855-378-0073
United Kingdom: +44 0800-917-2793
Singapore: +65 800-120-6718
Australia: +61 1-800-481-774
Japan: +81 0066-33-813303

About Symantec

Symantec Corporation (NASDAQ: SYMC), the world’s leading cyber security company, helps organizations, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec’s Norton and LifeLock product suites to protect their digital lives at home and across their devices. Symantec operates one of the world’s largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com, subscribe to our blogs, or connect with us on Facebook, Twitter, and LinkedIn.