

CPIQ

Consumer Privacy & Identity Quarterly

A Quick Look at Expedited Travel Programs

Confused by all the acronyms?
Here's a quick 101

It's All About that Baggage

How to manage your physical
and digital luggage

See ME See the World

A close-up look at the culture
of online travel sharing





DISCLAIMER

The Department of Defense (DoD) expressly disclaims liability for errors and omissions in the contents of this publication. No warranty of any kind, implied, expressed, statutory, including but not limited to warranties of non-infringement of third party rights, titles, merchantability, or fitness for a particular purpose is given with respect to the contents of this guide or its links to other Internet resources. The information provided in this guide is for general information purposes only. Reference in this guide to any specific commercial product, process, or service, or the use of any trade, firm or corporation name is for the information and convenience of the public and does not constitute endorsement, recommendation or favoring by DoD or the U.S. Government. DoD does not control or guarantee the accuracy, relevance, timeliness, or completeness of information contained in this guide; does not endorse the organizations or their websites referenced herein; does not endorse the views they express or the products/services they offer; cannot authorize the use of copyrighted materials contained in referenced websites. DoD is not responsible for transmissions users receive from the sponsor of the referenced website and does not guarantee that non-DoD websites comply with Section 508 (Accessibility Requirements) of the Rehabilitation Act.

In this Issue

4 Travel, Then and Now

5 Trending in Consumer Privacy News & Updates on Identity Technologies

6 A Quick Look at Expedited Travel Programs

7 Travel Savvy: Smart Accessories for the Modern Traveler

8 Cut the Lines: Can Face Recognition Ease Airport Anxieties?

9 It's All About that Baggage

10 Traveling in the Age of Mass Surveillance

11 See ME See the World

14 Close Encounters with Biometrics: A Traveler's Guide

16 Tired of Hotels? What to Know about Alternative Lodging

17 Test Your Knowledge

18 The Last Word

19 In the Next Issue... Online Gaming





Pre-Internet travel involved many unknowns. Tourists, adventurers, and long-distance commuters headed out to blank spaces on the map that only a small group of savvy sources could illuminate—travel agents, hotel concierges, and acquaintances who had visited before, plus maybe the occasional guidebook or brochure. It was difficult to know what to expect—what sights and amenities would be found upon arrival. It was challenging to keep in touch, access bank accounts, and make split-second itinerary changes. Once home, travelers could entertain family and friends with stories, or share printed photos or slideshows capturing what they saw and did. Still, it wasn't easy to describe the full magnitude of their experiences.

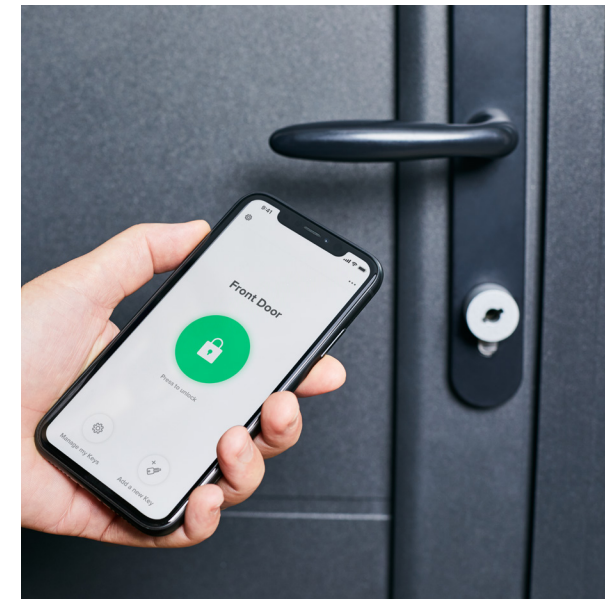
Today, thanks to an abundance of online trip planning resources, it's easier than ever for modern travelers to strike out on global adventures. Digital content shared by travel and tourism industry groups, localities, and prior visitors help prospective jet setters scope out every aspect of potential destinations, all before setting foot out the door. Online reviews offer detailed feedback and recommendations on restaurants, apartment rentals, and local experiences. A traveler can virtually walk their planned route using Google Maps Street View and browse tagged social media photos for any stop along the way. In short, travelers can be far more confident in their vacation plans.

Modern technology also streamlines travel. It acts as a safety net, helping share locations and trip updates for any interested loved ones back home, and providing a lifeline to travel resources (like airlines or rental agencies) or emergency services when needed. An array of smart travel accessories help charge devices, track luggage,

and extensively document trip activities. Advanced identification systems use biometrics to improve transit experiences. Today's travelers can live like natives in the communities they visit, thanks to online platforms for homestays.

Deliberately or not, each traveler adds their own small portion of digital data to the global travel information repository. Having taken advantage of online travel resources, travelers may feel an urge to report back—to share their own experiences and reflections for the next wayfarer—and may reveal key personal information in the process. Some may seek to translate their travels into online fame—using personal adventures to attract friends and followers on a global scale, without considering the privacy tradeoffs. Mandatory data collection also happens during travel. Biometric data can be captured at many points during a typical trip, and government agencies and travel companies alike collect detailed customer information.

This issue of CPIQ provides a quick update on travel programs and amenities for the unaccustomed traveler, showcases smart travel gadgets, and explores the privacy compromises involved with engaging in online travel communities. Along the way, articles discuss things each traveler can do to help keep their personal information, and that of family and friends, safe. This CPIQ also features a new "Trending in Consumer Privacy" section that recaps critical news and developments related to technologies discussed in previous issues. Read on to learn what the modern traveler needs to know about jet setting in an informed and privacy-protective manner.

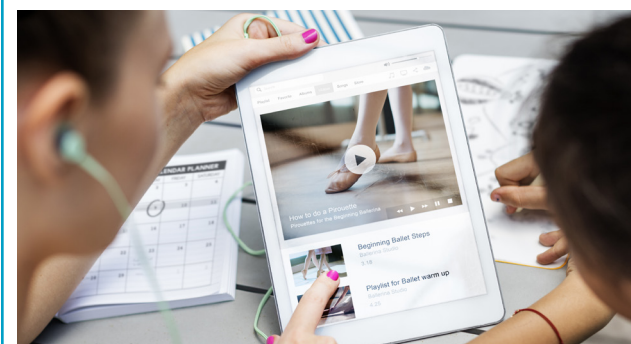


An Unexpected Technology Blends Physical and Digital Elements of Home Security

A new application of near-field communication (NFC) caught the attention of many tech journalists attending the January 2020 Consumer Electronics Show. Netatmo, a French company, debuted a smart lock system that offers physical keys (which act as NFC codes) that work with smart locks (NFC readers)—all of which can be programmed via a smartphone app. Users can configure a key to open multiple locks in a home or office, temporarily scale back or suspend a missing key's unlock privileges, or quickly conduct a digital lock change by resetting the NFC codes. This novel application of NFC may appeal to homeowners who are reluctant to try fully digital home security options.

Landmark COPPA Verdict Creates Complications for Content Creators

In September 2019, YouTube reached a substantial \$170 million settlement with the Federal Trade Commission (FTC) and New York Attorney General for breaching the Children's Online Privacy Protection Act (COPPA). Going forward, YouTube channel owners will need to specify whether their channel or any video content therein is directed to children per COPPA guidelines. Numerous content creators have voiced concerns over the proposed changes, as content with a "child-directed" label will not feature some of the popular interactive features—including notifications, comments, enhanced searchability, and viewing recommendations—that drive video and channel popularity.



Online DNA Test Kits are Off the Gift List

In December 2019, shortly before the start of the holiday season, the Pentagon released recommendations to military personnel to avoid using consumer-directed online DNA test kits. Online DNA services have become increasingly popular in recent years, helping users chart family ancestry and screen for potential genetic conditions. The Pentagon cited the industry's lack of regulation, particularly regarding how personal and genetic information is stored; unintentional leaks or breaches could put DoD personnel at risk for tracking or exploitation and compromise operations. Officials separately raised questions regarding the accuracy and reliability of online DNA tests in identifying key health issues.

A Quick Look at Expedited Travel Programs



Several trusted traveler programs launched in the last two decades aim to smooth identity verification and security checks. They promise time-saving convenience for travelers who are willing to complete voluntary prescreening, which may include background checks, interviews, and biometric data collection.

Looking to optimize your travel time? Here's a quick look at some U.S.-based programs:



TSA Precheck, run by the Transportation Security Administration (TSA), prescreens passengers for domestic air travel and logs traveler information into Department of Homeland Security databases. Passengers receive a known traveler number (KTN) that grants access to expedited TSA checkpoint screening lines and more relaxed security screenings (as the agents will remind you, "keep your shoes on!").

Several other programs ease international air and land travel between specific sets of countries, such as NEXUS (U.S. and Canada), and SENTRI (U.S. and Mexico). DoD members can often use their electronic data interchange personal identifier (EDIPI) number as a KTN to expedite air travel, though doing so will highlight their DoD affiliation.

Expedited travel programs can significantly ease the hassle of travel, but before signing up, be sure to consider the administrative organization, what personal data is collected, and how personal data is handled.



Global Entry, run by U.S. Customs and Border Protection (CBP), is available to U.S. citizens as well as lawful permanent residents and citizens of participating countries. Participants submit fingerprints and a photo during a CBP interview, and also undergo a background check. Qualified passengers can then complete ID verifications at automated kiosks while traveling, rather than with a CBP agent.



CLEAR is a privately managed registered traveler program that expedites screening at select U.S. airports and sports stadiums through fingerprint and iris biometrics rather than KTNs. CLEAR travelers can pass through security kiosks using biometrics, rather than having an agent inspect their ID and ticket.

TRAVEL SAVVY: Smart Accessories for the Modern Traveler

A traveler is only as "smart" as their travel accessories. See how today's cutting-edge devices and tried and tested gadgets can make for a smoother, more reassuring travel experience.

Smart suitcase

Using Bluetooth and a smartphone app, travelers can easily track their bag's location. Many also offer built-in USB charging.

Mobile hotspot

For use in almost any popular travel destination, this device transmits a secure, dependable Wi-Fi signal that can save travelers money on international cellular plans and data charges.

Clip-on smartphone camera lens

This camera lense conveniently clips onto a smartphone to provide enhanced optical zoom, helping users capture high-quality close-up shots from a safe distance.

USB flash drive

USBs help store secure copies of identity and travel documents, in case the originals are stolen or misplaced. Just make sure to encrypt and/or password-protect saved files.

Portable charger

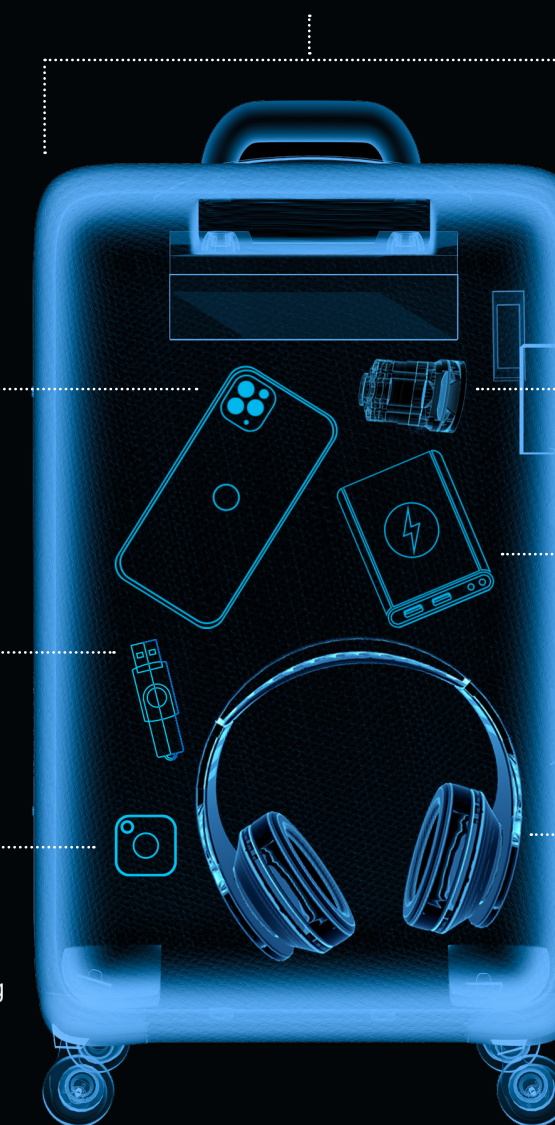
Avoid having to hunt for an outlet. This essential carry-on item holds enough battery power to fully charge a smartphone multiple times, helping make travel delays slightly more tolerable.

Bluetooth trackers

It's easy to lose or misplace items when on the go. A Bluetooth tracking device can be attached to any essential travel items, so they can be easily located using a simple smartphone app.

Wireless headphones

Travelers trying to cancel out unwelcome noise can also keep their ears warm in the chilly airport boarding area with these state of the art, foldable wireless headphones.



Cut the Lines:

Can Face Recognition Ease Airport Anxieties?



People everywhere can relate to the frustration of waiting in lengthy airport lines. Passenger queues define the airport experience. There are lines for everything—from check-in, to security, that one good coffee stand, and boarding. Since, according to a September 2019 article from NEC (an information technology company), the number of air travelers is expected to double by 2030, this frustration is likely to grow. However, the ease and efficiency of facial recognition (FR) in ticketless travel promise to greatly reduce dreaded airport backups and give way to a new age of global travel.

FR technologies enable passengers to access ticketless boarding, putting control over the pre-travel experience firmly in their...faces. Scanners pick out passengers' unique facial features, which map to digital profiles that connect to boarding passes and travel documents such as passports.

Among several far-reaching benefits, ticketless travel can significantly reduce flying stress and improve the overall passenger experience. In 2016, a company in Singapore utilized FR technology in a transport ticketing system that automatically identified and charged passengers passing through the premium ticket gates. Other ticketing systems let passengers use FR on their smartphones to simplify the purchase process.

While convenient, FR presents some unique risks. Careless travel companies and abusive employees could potentially leak or access personal biometric data, which could, in turn, be used maliciously. Additionally, government agencies (both foreign and domestic), could potentially use FR to precisely track travelers. As part of the biometric

entry-exit program, U.S. Customs and Border Patrol (CBP) requires U.S. citizens to undergo facial recognition during boarding and re-entry. While the CBP insists the program is not intended for surveillance purposes (the agency does not keep long-term facial images, and U.S. citizens can opt-out if desired), the agency rolled out FR technology in airports before gaining large-scale public awareness or buy-in.

Several major airlines in the U.S. are including the CBP's facial recognition technology in routine security processing. At the end of 2018, in cities such as Atlanta, Detroit, and Minneapolis, Delta Air Lines joined up with the CBP and the Transportation Security Administration (TSA) to implement facial recognition checks throughout international terminals, with other airlines like JetBlue and British Airways following suit. Also, in 2018, United Airlines started testing facial recognition technology for international travel at airports in Houston, Washington, D.C., and San Francisco. Both Delta and United are working with CLEAR (a private registered traveler program) to apply a biometric security option across some of their airport hubs. American Airlines also kicked off a trial program at Los Angeles International Airport in 2019 to evaluate FR identification for pre-boarding.

Looking ahead, it's difficult to gauge what personal tradeoffs travelers will be willing to accept. Airport-goers will need to consider what entities collect face data, how it is shared, and how it is linked with payment and security systems. Today, global travelers still have the power to opt-in or out, but the "no lines" experience FR promises may be too convenient to pass up.

It's All About that Baggage

Keeping track of luggage can be a hassle, but do you consider your digital baggage too? Digital baggage consists of data on any of your travel devices, plus data you generate via social media posts, restaurant or ride-share reviews, and other online activities. Either type of baggage can reveal a great deal about your identity and travel plans, but there are steps you can take before, during, and after a trip to reduce risk exposure.

Prep carefully

Physical: Before setting out, conduct a baseline condition check on your luggage. Ensure all zippers and closures work and remove old bag tags and prohibited items. Remember that travel clothing and gear can hint at your destination and planned activities.

Digital: Consider bringing a secondary laptop or smartphone instead of your primary devices. Only install the apps and accounts that you will need for your trip, as this limits risk if your device is lost or hacked.

Be proactive on the go

Physical: Keep track of your luggage—some consumers use Bluetooth tags to map their bags' locations. Pack and use luggage locks if you're uncertain about security at your destination.

Digital: Disable Wi-Fi and Bluetooth connections while in transit (even shopping kiosks can capture and log your device identifiers). Do not connect your devices to public USB ports, unless using a power-only adapter that prevents malicious data transfer.

Tidy up

Physical: At your destination, inventory your packed belongings and safely discard used tickets and luggage stickers (consider shredding these items).

Digital: Scan your devices for malware before re-connecting to your home networks, or conduct a device reset. Consider updating the passwords for any accounts and services you accessed during your travels.

There is no exact formula for flawless baggage management, but taking a proactive stance can help avoid unwanted situations. Be sure to share best practices with your travel companions.



Traveling in the Age of Mass Surveillance



Modern travelers are reaching more destinations around the world than ever before. According to the World Tourism Organization (UNTWO), a record-breaking 1.4 billion international tourist arrivals occurred in 2018. While the expansion of global tourism arguably offers many benefits, international travelers are particularly vulnerable to surveillance and data breach threats as they navigate new environments with unfamiliar regulations and risks. Consequently, international trips come with responsibility for extra security and privacy considerations.

Understand the laws in your destination country

The first step to protecting yourself is to read up on the laws of the countries you are planning to visit. Some countries are known to monitor and surveil information from their IT networks, such as China, Russia, and Belarus. The U.S. State Department went so far as to issue an advisory during the 2014 Sochi Olympics, which stated: "Travelers should be aware that Russian Federal law permits the monitoring, retention, and analysis of all data that traverses Russian communication networks, including Internet browsing, email messages, telephone calls, and fax transmissions." If you plan to travel to one of these destinations, leave your everyday devices at home and consider bringing a dedicated burner phone for the trip to prevent your detailed digital footprint from being compromised by foreign government surveillance.

Also, it is crucial to check if using encryption and virtual private networks (VPNs) is legal at your destination. In addition to the three countries above, Burma, Hungary, Iran, Israel, Kazakhstan, Moldova, Morocco, Saudi Arabia,

Tunisia, and Ukraine all require a special permit or license to bring encrypted devices into the country, even for personal use. This means if you arrive with an encrypted laptop and no prior authorization, you may be fined, and your computer confiscated. If foreign customs agents review your laptop or storage device during your travel, assume its content has been breached and take steps for remedy as needed, such as updating account passwords.

Be aware of public security cameras

The proliferation of closed-circuit televisions, or CCTVs, expose travelers to the risk of being involuntarily recorded on video while conducting typical tourist activities. Both federal and local governments are installing CCTVs at exponential rates thanks to the ease with which they can be integrated into smart security systems. For example, the U.K. has deployed over 6 million CCTVs cameras nationwide, and China is expected to install over 567 million cameras by 2021. While CCTV surveillance began as a simple tool for supporting criminal justice, the technology has advanced enough to integrate sophisticated face recognition (FR) and artificial intelligence (AI) software for advanced behavior forecasting and crime detection. As smart security networks expand and connect, the chances of an innocent traveler not being caught on camera seem lower than ever.

As technology brings both our physical and digital worlds closer together, modern travelers face new privacy challenges. Fortunately, safeguarding privacy is still possible if you take time to research potential risks before you travel.

See *ME*

See *the world*

You cannot believe your eyes as you look skyward and see the tallest man-made structure ever built. Thoughts of soaking in the moment or making a sketch of the precipitous heights soon give way to grabbing a selfie stick, taking a shot, and posting the photo on Instagram and Snapchat to forever commemorate and share with the world the moment you first witnessed the Burj Khalifa in all its glory. Next, you eagerly anticipate how many likes and views this post will get you.



Prior to the advent of the Internet, travel was a more personal and private endeavor. Once on the road, vacationers were nearly unreachable, their precise locations unknown. Disconnected from society, they were free to fully live in the moment. Trip documentation was limited to pen and paper, or to a roll of film that may, or may not, capture spectacular memories.

Contrast that to the current digital age, which supports a robust cultural impulse for modern travelers to share every vacation detail on social media. According to a 2019 article by *Travel Mindset* that described Instagram’s impact on the travel marketplace, approximately 97% of vacationing millennials post to social media—sharing photos, videos, live streams, songs, and podcast recordings—to document and share their travel experiences with friends, family, and the public. Nearly 260 million pictures are publicly indexed and tagged with #travel just on Instagram alone. Social media services also help travelers continuously broadcast their exact locations, keep in touch via messaging, and connect with new friends—activities that expand and enrich social networks and digital footprints.

According to a fall 2019 article from Sparkloft Media (a social media agency), approximately 3.5 billion people actively use social media to connect with family and friends as well as brands they are interested in. Travel and tourism industries have led the way in developing niche social media circles, with groups formed by brands targeting specific audiences to discuss travel plans, interests, and recommendations on trip essentials such as lodging and dining options. Take, for example, the Facebook group “It’s Orlando Time,” consisting of

travelers from the United Kingdom. The group maintains hundreds of thousands of followers, logging nearly 1,000 daily posts about traveling specifically to Orlando, Florida.

With endless opportunities to share and learn on social media, travelers plan destinations according to whether the trip is “Insta-worthy” and will subsequently enhance their social networking experience. According to a recent social media survey conducted by Instagram researchers, roughly 40% of travelers base their travel destinations on the “Instagrammability” of that particular place—whether it is photogenic enough to deserve a post on social media, and if it will inspire a desirable level of envy among viewers.

Has online sharing emboldened people to travel more in the first place? Or to pursue experiences they may not have otherwise considered, just for the sake of attention or online social gratification? Does travel sharing give us some influence over others when it comes to the global travel experience? Recent studies suggest that social media has increased the impact of user-generated travel recommendations, as modern travelers regularly seek out social media for travel inspiration and personal validation. The power of social media and “selfie culture” is depicted in an early 2019 survey conducted by Stackla through the following statistics:

- 86% of people claim to be more interested in visiting a specific location after seeing user-generated content
- 60% of people view user-generated content as the most influential when planning travel (when compared to professional brand images and celebrity-influenced content)



Have you ever found yourself looking at friends’ travel photos on social media and wondering if the destinations actually look that good IRL (in real life)? It’s not just you—there’s a decent chance those stunning photos and videos in your feed have been edited to draw out the perfection of the scenery or the vividness of the user’s experience.

For example, the Visual Supply Company (VSCO) app that launched in Oakland, CA in 2011 is one of many photo and video editing tools that provide preset filters for professional-quality photo editing and enhancements. These apps encourage users to creatively express themselves through content editing and then share the resulting content via social media. According to a December 2019 *TechCrunch* article, VSCO will likely reach four million paying users in 2020, most of whom are age 25 and younger.

Interestingly, popular social media sites view third party media enhancement apps as collaborators in marketing content—including travel products, services, and destinations—to users. In late 2019, for example, Snap Inc. partnered with VSCO to create Analog, a unique, limited-time Snapchat lens consisting of multiple filters highlighting the perfectly imperfect mishaps that occur in video filming.

Today, media editing and enhancement apps can offer premium payoffs in helping build social networks and followers. Ambitious and tech savvy travel influencers are probably taking advantage of some of these apps to expand their online allure. If you’re vacation planning online, try to remember there may be a slight disconnect between content featured in popular destination posts and what you see IRL once you arrive.

- 52% of travelers have made plans to visit a specific destination based on personal posts from friends, family, or other social media peers

These trends have prompted some to argue that our current travel culture, sometimes described as “narcissistic” or rooted in “FOMO” (fear of missing out), are ruining the travel experience. The need of the modern traveler to be liked and validated is evident in typical posts—such as a picture of an exotic beach captioned, “Are you jelly?” Gone are the days when having just a journal and camera was sufficient to enjoy a trip and make lasting memories. Now, travelers feel the need to publicize everything they do in the moment, and at least have it appear to be “the absolute best thing ever!”

Likes aside, travelers may also be sharing too much for their own good. Social media can be a hunting ground for fraudsters targeting a traveler’s personal information. Oversharing can leave a detailed trail of trip locations for potential hackers and identity thieves to follow. Bad actors can exploit a traveler’s sensitive financial information over public Wi-Fi, or take over a user’s social media account in an attempt to scam friends and family members out of money (a modern take on the classic “traveler in distress” scheme). Posting status updates, upcoming travel plans, and even tagging other vacationers on the same trip can jeopardize personal information. Another risk of oversharing on

social media concerns the potential negative impact on children. Overall, more parents than children use social media while traveling, and any information shared about kids’ lives can lead to an invasion of their privacy and even cyberbullying.

Travelers should always be mindful of the personal information they share online in order to protect themselves and loved ones from unnecessary scrutiny and cyber threats. Some social media best practices to keep in mind:

- Don’t share flight or transit information
- Wait until arriving home to post vacation photos
- Take proper precautions to secure accounts—possibly through the use of a VPN (virtual private network) to disable location and IP address tracking
- Practice content moderation, and limit check-ins, live streams, and real-time reviews

Finally, travelers should remember that sharing digital trip data creates a permanent record that becomes accessible for future viewers, who could range from grandkids to prospective employers. One must consider whether today’s likable travel shares are going to be equally well-received by future audiences. Will they think that wild and crazy trip to the Buenos Aires Carnival exemplifies living life to the fullest? Or fully (and senselessly) oversharing?

CLOSE ENCOUNTERS WITH BIOMETRICS: A TRAVELER'S GUIDE



Check-in

The traveler checks in online or at an automated kiosk. The system captures the user's face to compare and verify against official identification documents (such as a passport), without input from an airline employee.



Bag Drops

The traveler creates luggage tags by using face authentication at a bag drop kiosk. They label their bags and drop them at the designated location.



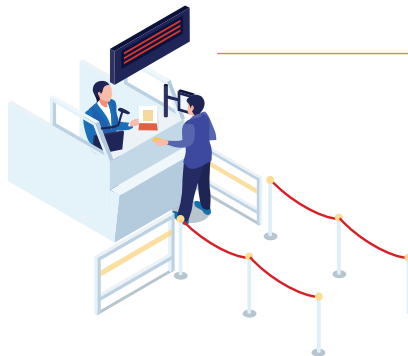
Security Check

Instead of presenting a boarding pass and physical ID to security personnel, the traveler shows their face to cameras placed at the security checkpoint. The captured image is used to verify the traveler's identity.



Boarding

The traveler authenticates their identity and enters the plane by presenting their face to a camera near the boarding gate, rather than presenting a boarding pass to an airline attendee.



Immigration - Entry Screening

If traveling internationally, border control agents or kiosks may collect face, iris, or fingerprint data to record the traveler's entry into the destination country.

Biometric technology is everywhere, from our smartphones to airports, and spread throughout the cities we visit. As a result, modern travelers are increasingly relying on biometrics instead of IDs or passports to verify their identities. How many points during a journey might a traveler potentially encounter biometric technologies? Let's find out.

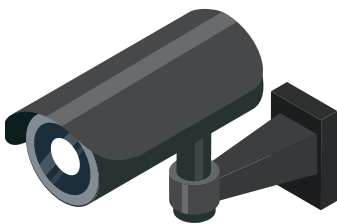


Car Rental

Rather than dealing with car rental agents, the traveler unlocks a rental car using biometric authentication on their smartphone and exits the rental car garage by looking at a camera located near the exit.

CCTVs (Closed-circuit television)

CCTVs (camera networks installed across cities and properties for crime surveillance) are prevalent in countries around the world. For example, over 7,300 cameras are installed in Seoul, South Korea's capital. These devices may record the traveler's face and movements.

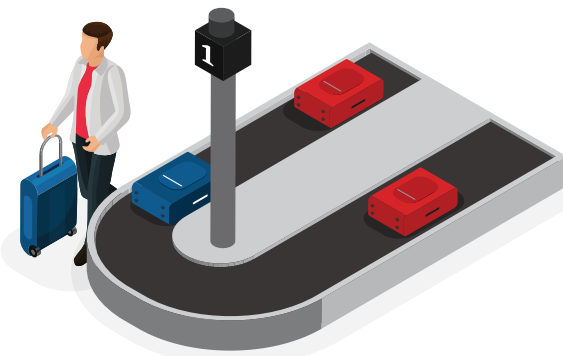


Immigration - Exit Screening

The traveler verifies their departure from a country by submitting required biometrics, which are matched against biometrics collected during entry. The traveler's biometric data is deleted upon departure.

Automated Passport Control (APC)

The traveler skips manual passport control and proceeds to an APC kiosk to answer customs questions and submit their face for biometric verification.



Baggage Claim

The traveler authenticates on their smartphone to receive real-time baggage processing updates and collect their luggage from baggage claim. Home sweet home!





Lodging is one of the most significant vacation expenses. Luckily hotel alternatives abound, offering cheaper and occasionally more convenient options than typical \$200-a-night hotel stays. But for the price cut, what types of privacy and security trade-offs are you making?



Vacation Rentals

Barcelona apartments and Caribbean beach houses are available to reserve short-term with vacation rentals services like Airbnb, VRBO, HomeAway, and 9flats. Vacation rental sites help hosts open up

privately maintained homes to guests while providing travelers with authentic local experiences.

Pros: Access a variety of lodging types—from renting a room in someone's apartment, treehouse, or an entire mansion—depending on your needs and budget. Kitchen access can help save money on restaurants.

Cons: Lack of regulation means travelers have minimal rights. Once your stay is reserved, the host can request additional documentation, such as a scan of your passport or visa. With Airbnb, your apartment may come with interior security cameras that can record you. Review the listing carefully for camera disclosures, unless you like being surprised. Lastly, vacation rentals offer less flexibility, as cancellations require more advanced notice than hotels.



Specialty Housing

Services like Monastery-Stays and UniversityRooms connect travelers to available rooms in local dormitories at a discounted rate.

Pros: Enjoy the security and structure of staying with an established

organization, without the hotel price tag.

Cons: Don't expect luxury and frills—your room will be clean and functional, but without extra perks.



Homestays

For the adventurous, homestays provide the cheapest lodging option. Services like Couchsurfing and Servas International connect travelers with a spare room or an open couch.

Pros: Cost—it's minimal or free in many cases. It is also a great way to meet locals.

Cons: You are at the complete mercy of the host. Always read reviews of the host before opting in for the bargain price.

Test Your Knowledge



- It is important to encrypt and password protect files stored on which of the following smart travel accessories?
 - Bluetooth tracking devices
 - USB flash drives
 - Mobile hotspots
 - Smartphone camera rolls
 - Bluetooth headphones
- For the modern traveler, which of the following is not a risk associated with oversharing on social media?
 - Getting too many likes on trip photos posted to social media
 - Cyberbullying or invasion of a child's online privacy
 - Leaving a trail of trip locations and personal information for hackers to exploit
 - Malicious actors scamming friends and family members out of money
 - Having other social media users reshare your posts to unknown audiences
- Which of the following has not been identified as a benefit of FR in ticketless travel?
 - Less wait time in airport security lines
 - Simplified purchasing processes
 - Public disclosure of biometric data
 - Reduced flying stress
 - Less wait time in baggage drop lines
- In which of the following scenarios would a traveler potentially interact with biometric technology?
 - Checking into a hotel
 - Renting a car
 - Shopping in the duty-free store
 - Asking for directions
 - Purchasing beverages in a transit terminal
- Which of the following are potential risks to consider when staying at a hotel alternative?
 - Being recorded by hidden security cameras
 - Experiencing difficulty in making last-minute reservation changes
 - Having to digitally share ID documents with the host
 - Having to deal with a difficult or unpleasant host
 - All of the above
- As a privacy-savvy user, which of the following would you do while traveling a foreign country?
 - Use public Wi-Fi as much as possible
 - Bring and use a dedicated burner phone for the trip
 - Download as many local apps as possible
 - Create posts in real-time to share with your social media followers
 - Use public USB charging ports to charge your devices
- Travelers in airports cannot be identified by:
 - Bluetooth-enabled sales kiosks
 - Public Wi-Fi connections
 - Airline luggage stickers
 - Duty-free shopping forms
 - Retail cash purchases
- Which of the following expedited travel programs is not managed, at least in part, by U.S. government agencies?
 - TSA Precheck
 - Global Entry
 - NEXUS
 - CLEAR
 - SENTRI
- In order to maintain COPPA compliance, YouTube content creators have been instructed to apply "child-directed" labels to kid-oriented content. Child-directed videos will not have which of the following features:
 - Notifications
 - Comments
 - Enhanced searchability
 - Viewing recommendations
 - All of the above
- True or False: It is legal to bring an encrypted device into any foreign country if the device is intended for personal use.

The Last Word

For the modern traveler, getting out and seeing the world may not be sufficiently satisfying. Today’s technology allows us to carefully research, document, and share our travel experiences with curious acquaintances as well as the public at large. Whether you’re passing along advice for the next visitor, or humble bragging about your “long weekend” in Italy, remember to consider whether sharing trip details of any kind will benefit your overall digital privacy—both now and in the future.

Vacations are ideal times to check-out from daily hassles, but it’s especially critical to maintain a privacy-protective mindset while traveling. Be smart about how you manage your baggage (both physical and digital!) while on the road, and take whatever time is necessary to educate yourself about privacy and safety risks that may impact you in transit or at your destination. Whether you’re hitting the beach, the trail, or busy city streets, there are many proactive steps you can take to keep your personal information safe—no one wants to return home to a compromised identity.



In the Next Issue...

While not without controversy, video gaming has become an important and vibrant part of global mainstream entertainment and culture. During the last several decades, video games have transformed from standalone arcade consoles to heavily networked, immersive environments that players can access anywhere with an Internet connection.

The next issue of CPIQ will illuminate the technical history of video game development, explore the new social aspects of gaming, and introduce key components of modern gaming for any prospective n00b (new) players. Readers will learn why more people are embracing gaming and how to keep personal information safe while enjoying this thriving form of digital entertainment.



For more detailed information on protecting and managing other key elements of your identity footprint online please check out the:

IDENTITY AWARENESS, PROTECTION, AND MANAGEMENT GUIDE

A GUIDE FOR ONLINE PRIVACY AND SECURITY COMPRISED OF THE
COMPLETE COLLECTION OF DEPARTMENT OF DEFENSE SMART CARDS
EIGHTH EDITION, MARCH 2019



BROUGHT TO YOU BY:



U.S. DEPARTMENT OF DEFENSE

IDENTITY AWARENESS, PROTECTION AND MANAGEMENT GUIDE