ISSUE 001 UNREDACTEDMAGAZINE.COM MAY 2022

UNREDACTED

COMMON LAW NAMES & COVER ID

CAN YOU LEGALLY OBTAIN AN ID IN AN ALIAS NAME?

EMAIL IS BROKEN

AND THERE'S NOTHING WE CAN DO ABOUT IT

LEAVING AMAZON KINDLE

ALTERNATIVE READERS WHICH DO NOT TRACK YOUR READING

OSINT TIPS

HARD REFRESHES, UTILITIES SEARCHING, AND MORE

CONTENTS

UNREDACTED is published free of any charge to the reader, and this file may be publicly shared in its entirety. All issues are available for free download at https://UNREDACTEDmagazine.com. Contact details are also available at this site.

Cover Design by Anonymous Reader. Special thanks to everyone who helped make this happen. You know who you are.

FROM THE EDITOR

By Michael Bazzell

Thank you for downloading the first issue of UNREDACTED Magazine. The idea of a privacy-related periodical has been brewing in my head for some time. I already have a weekly podcast which has been a great outlet for updated content to my books, but podcasts are not always ideal. Many people simply do not have the time to ingest an hour of audio every week. Podcasts are also not great for referencing past spoken material. Telling someone to listen to minute 42 of episode 84 to learn about a technique usually results in a missed opportunity.

This free magazine in searchable PDF format tries to solve these issues. It can be read online or offline, and archiving is easy. It is a throwback to a time when we focused on a single task which didn't involve numerous browser tabs screaming for our attention.

My goal is to provide valuable text content over anything else. I don't want flashy graphics and color-coded segments on every page. I don't need breakouts to tease upcoming articles or issues. While I call this a magazine, it feels more like a series of whitepapers. The layout may seem very plain, which is somewhat intentional.

I have borrowed heavily from the overall concept of 2600: The Hacker Quarterly. For many years, I rushed to a local book store to pick up the latest copy of 2600 and then read it cover to cover that same day. I digested every word as if each were secrets to finding buried treasure. 2600 still exists, but it rarely touches the topics of privacy, security, and OSINT, and the content has deviated from its roots. I want UNREDACTED Magazine to fill that void.

While I will contribute to every issue, I want the focus to be content from readers. I have two current books available which provide plenty of my own ramblings. I want the true value of this publication to be the views of others. I also want this to be a product which I look forward to reading. By incorporating several articles from various internet strangers, you and I both get to enjoy the content together. I will always strive to make sure each issue is something we are both excited to read.

You will notice the presence of advertisements (sponsors) within each issue. This was intensely debated. While the financial costs to create and distribute this digital product are minimal, the time requirement of my staff is substantial. I insisted we offer this magazine for free under a Creative Commons license. My goal with sponsors is to justify the time and expense while breaking even at the end. I refuse to place ads on my podcast because I want to eliminate any potential bias within my own voice. Since the majority of this magazine's content is provided by others (who have no information about any ads until after publication), I feel that ads are acceptable when properly labeled. However, I will always insist that any ads be directly related to the products we use and recommend. You will never see an ad for Facebook or Google here.

The most important piece to make this project work is you. Contributions by readers are the heart of this product. If you would like to be a part of this project, please consider contributing an article, review, question, letter, update, or anecdote. More details about these submissions can be found at UNREDACTEDmagazine.com. If you prefer not to be involved, spreading awareness of the project is just as valuable. Give out the PDFs. Send people a link. Bring others into our world.

This first issue will be rough in spots. The layout may seem amateur. It will take us some time to find our way. However, I promise each issue will display obvious progression as we improve. If you have talent related to magazine layouts and want to be involved, please contact us. Remember, this is a free community project. We will need help to make it to the next issue.

I ask that you take your time reading through this magazine. Our peers have put a lot of thought and effort into their submissions. Please embrace the PDF magazine format and appreciate the benefits of the technologies which allow us to work together globally to strengthen our privacy and security strategies. I hope you receive as much enjoyment from these issues as I know I will. Thanks for being here.

~MB

EMAIL IS BROKEN AND THERE'S NOTHING WE CAN DO ABOUT IT

By AmIJesse

Email is coming up on its 50th birthday, and while better than it used to be, it's far from perfect. One problem with using something invented before the internet as we know it is that it wasn't built with security in mind, it was simply used for sending messages and files to other computers on the same network. Fast forward to today and everyone is under constant attack by malicious actors trying to profit off of us. Not wanting to break backwards compatibility we haven't made any major changes to how email really works. Unfortunately, this means bolting security measures on top of existing features and hoping that everybody follows along. There are three main methods we use nowadays to verify an email sender: SPF, DKIM, and DMARC.

SPF: SPF (Sender Policy Framework) was the first to officially be adopted and is most commonly used today. It relies on existing DNS (Domain Name Service) technology to verify that the sender of an email is actually allowed to send the email. To check any domain's SPF records you just need to conduct a TXT lookup on the domain. As an example, UNREDACTEDmagazine.com has the following record (you can look for yourself at https://mxtoolbox.com/txtlookup.aspx):

```
Type: TXT
Domain: unredactedmagazine.com
TTL: 30 Min
Record: "v=spf1 include:_spf.protonmail.ch mx -all"
```

Reading the record may be a little confusing, but let's step through it piece by piece. **v=spf1** tells us that we are using SPF version 1 (the current standard). **include:_spf.protonmail.ch** allows ProtonMail to send emails on our behalf. **mx** allows any servers we specify in our MX records (which you need to send and receive emails) to send emails for us. **-all** describes what we want done with emails that don't match any of our previous servers. There are multiple possible entries that you might see here, they are "-all" (reject all emails sent that don't match), "~all" (accept the email, but flag it as suspicious), "?all" (it may or may not be valid), and "+all" (accept all emails as valid) which is never recommended.

DKIM: DKIM (Domain Keys Identified Mail) is a way that mail servers can cryptographically sign outgoing emails, and the receiving server can use the DKIM entries to verify the signature. There isn't much here that's important for us to know, and you will just add the domain CNAME records that your email provider tells you to.

DMARC: DMARC (Domain-based Message Authentication, Reporting, and Conformance) is where security starts to get real. By adding a TXT record to "_dmarc.yourdomain.com" you can tell mail servers what to do with emails that don't match your previous records (SPF and DKIM) and what to do in the case someone tries to spoof your email. The biggest benefit to DMARC over SPF is that it's domain wide, where SPF is specific to any subdomain you add the record to. We will use UNREDACTEDmagazine.com as an example again. You can search it at https://mxtoolbox.com/txtlookup.aspx and receive the following:

```
v=DMARC1; p=quarantine; fo=1;
rua=mailto:dmarc@unredactedmagazine.com;
ruf=mailto:dmarc@unredactedmagazine.com
```

This record might look even more confusing than SPF, but if we step through it piece by piece it will start to make sense. **v=DMARC1** specifies the version of DMARC we are using. **p=quarantine** is similar to our final SPF record we looked at, and just like it there are different values you may see depending on what the domain owner wants to do with emails that fail validation. The three possible values you may see are "p=none" (don't take any special action, but use it for reporting (more on that later)), "p=quarantine" (allow the email to go through, but send it straight to the spam folder and flag it as suspicious), and "p=reject" (drop this email immediately without completing the send). With all policies, metadata is saved to be reported to the domain owner if they want to receive reports. **fo=1** is your failure reporting option, of which there are 4 possible values. "fo=0" (only send a report if both SPF and DKIM fail validation), "fo=1" (send a report if either SPF or DKIM fail validation), "fo=s" (send a report if SPF fails), and "fo=d" (send a report if the DKIM signature fails validation).

rua=someemail@domain.com specifies what email address to send reports about SPF and DKIM checks to. RUA emails are generally sent once a day, and don't contain any PII about the spoofed email. **ruf=someemail@domain.com**

specifies what email address to send reports to. The only difference being ruf reports will send quite a bit more PII about the spoofed email, unfortunately most mail services don't support ruf so this one can be omitted without worry.

If you want to send your DMARC results to an email at a different domain than it's reporting on there's one more step you need to take. Let's say I want to send all records on hastysec.dev to jesse@buffer1024.com instead. I would need to create a TXT record on buffer1024.com with a host of "hastysec.dev._report._dmarc" with a value that looks like the following.

```
Type: TXT
Domain: hastysec.dev._report._dmarc.buffer1024.com
TTL: 30 Min
Record: "v=DMARC1"
```

Where's the problem? Now that we have a good idea about how emails are protected let's go over some problems with it. The main problem we're going to cover here is that every mail provider handles the sender verification process in a different way, and even recommend different settings when guiding you through setting up your own domain. This is a major problem because it means we can never know that our emails aren't being spoofed even if we've done everything right. All it takes is one insecure email service and everyone who uses it is a potential victim. The onus is on the receiving mail server to determine if the incoming email is valid.

If you are setting up your own domain, or have previously set up your own domain, be sure to add all three of the previously mentioned records even if your mail host doesn't require you to. We will prove to you why by the end of this article.

The anatomy of a spoofed email: While this isn't intended to be a guide on how to spoof emails, covering how spoofing an email works is integral to understanding the rest of this article. For this example, we are going to try to spoof an email from "admin@google.com" to "user@google.com". The first step is to figure out what mail servers the receiving user is using. We can simply look on mxtoolkit.com again by searching google.com.

```
Pref    Hostname                  IP Address
8       smtp.google.com           172.253.115.26
8       smtp.google.com           2607:f8b0:4004:c06::1a
10      aspmx.l.google.com        172.253.122.
10      aspmx.l.google.com        2607:f8b0:4004:c06::1b
20      alt1.aspmx.l.google.com 209.85.202.26
20      alt1.aspmx.l.google.com 2a00:1450:400b:c00::1b
30      alt2.aspmx.l.google.com 64.233.184.26
30      alt2.aspmx.l.google.com 2a00:1450:400c:c0b::1a
40      alt3.aspmx.l.google.com 142.250.27.26
40      alt3.aspmx.l.google.com 2a00:1450:4025:401::1a
50      alt4.aspmx.l.google.com 142.250.153.26
50      alt4.aspmx.l.google.com 2a00:1450:4013:c16::1b
```

The "pref" column specifies the order you should try sending mail to the servers, starting at the lowest and working your way up. The hostname or IP address is all we really care about. Now that we know the mail server's hostname, we can connect to the mail server and start sending it "commands". Note: you will need to be allowed outgoing connections on port 25. Most home ISPs and VPS providers don't allow this as it can be used to send spam emails. I don't recommend doing this from your workplace either, as it can end up with your IP address on some blacklists.

As we can see by the message at the bottom of image 001 at the end of this article, DMARC worked and blocked the email before it ever touched the user's inbox. We will play around with this a bit more later on, for now let's cover what we did. Everything we need to type is labeled with a number and I'll explain each command.

1. "telnet smtp.google.com 25" opens a connection to smtp.google.com on port 25. This does not need to be run as root, and shouldn't be, this is just a test server so it doesn't really matter.
2. "HELO localhost" sends a "HELO" command with your domain as an argument. The domain isn't verified during this connection, but is used for spam/spoofing detection, so it's recommended you point a domain to the machine you're spoofing from and use that domain instead of localhost.
3. "MAIL FROM: <admin@google.com>" is the email that will be used as the sender of the email (this is what SPF/DKIM and DMARC are checked against), and is what the mail server refers to as "envelope_from".
4. "RCPT TO: <user@google.com>" is the person you are sending the email to.
5. "data" tells the server we are going to start entering the email data (headers, then email body).
6. *header data separated by newlines* is where we enter the headers the email will contain. The RFC (linked below) specifies the "To" and "From" headers as required, but only some mail servers actually care if they're included. The headers you choose to use are important to bypassing spam filters, as most spoofed/spam emails don't use optional headers. More on that later.

7. "*newline* Spoofed Email" is where we enter the body of the email. There needs to be a blank line between the headers and the start of the message body.
8. *End of email* When you're done sending the body, enter a newline, then a period, then another newline.
9. Tell the mail server we're done.

For more information on email specifications, you can read the RFC at https://datatracker.ietf.org/doc/html/rfc5322. If you want to start bypassing spam filters, finding new methods, it's recommended you at least skim over it and look at the different optional header fields.

A commonly used method of email spoofing, involves configuring your domain's SPF/DMARC to allow your spoofing IP to send email. Then using that valid domain in the "MAIL FROM" message, and just modifying the "From" header to be the spoofed email. Mail providers have caught on, and you don't really see these emails getting through often, as it's a pretty big red flag when those to values don't match.

A working example: On the one hand, I hesitate to show exactly how to get a spoofed email into a user's inbox. On the other hand, attackers are going to figure it out on their own, and it won't hurt for the rest of us to know what to look for. In this example, I'm going to target a Tutanota user (my own inbox). I want to make it clear that the only reason I'm singling them out is that they actually handle SPF fails "properly", while still allowing messages to reach the inbox fairly easily. Two other popular secure/private email providers I tested do not (at the time of this writing) notify the user if an incoming email has failed the check.

This time we're going to send an email from a domain I own, to my newly created Tutanota email. On the spoofed domain our SPF record is set to only allow ProtonMail to send my emails, and "~all" set as the default SPF rule (let the receiving server determine how to handle the matching fail, but it's probably spoofed). We don't have a DMARC record on this domain (at the time of this writing).

First, we're going to start out the same as we did in the Google example - get the mail servers for tutanota.com (mail.tutanota.de). Then following the same routine as last time, spoof an email to my inbox.

Looking at my inbox, I can see I indeed did receive the email directly into my inbox. There was a nice banner notifying me that the sender probably isn't valid, now let's see what happens if we try to spoof an email from a domain with DMARC configured. Image 002 on the last page displays the result. This time Tutanota sent it directly to the spam folder though. There are ways to show the email in the inbox on some mail providers, but I'm not going to go into details as I've reported the issue and want to wait for it to be fixed.

Email is truly broken: But wait, the last time we tried to spoof admin@google.com we got a DMARC failed message. Why did it go through this time? This is where we start to see some major inconsistencies in how mail servers handle incoming mail. While google does a lot to check that incoming mail is really coming from where it claims to be, a few notable others don't do nearly enough.

Out of the major email providers I tested, Google, Hotmail/Live/Office 365, and Yahoo (what year is it?) have the best response to spoofed emails by far. Any incoming mail that fails SPF immediately go to spam. If DMARC is configured on the spoofed domain the emails get dropped and don't even make it into spam. Tutanota is the next safest when handling SPF fails, adding a warning banner on any email that seems suspicious, but still allowing DMARC fails to hit the spam folder.

That leaves us with ProtonMail and Fastmail. Unfortunately, they are both currently lacking protections that the previously listed all have. Within a day of starting my testing I was able to get an SPF and DMARC failed message into both inboxes, without any notice that the email may have been spoofed in the case of Fastmail.

Naturally, I sent an email to the effected mail providers about the issue. ProtonMail got back to me asking for more information and hopefully we can expect a fix soon. Interestingly, Fastmail claimed that they don't consider it a security issue. After asking for clarification they said that it isn't eligible for their bug bounty, so I should email their support team about it. Of course I still reported the bug to their support team. After all, it's up to people like us who find security problems to report them before they can be used against us.

Now we get to the real problem of email. Fastmail refused to change anything on their end because it could negatively affect users who haven't properly configured their domains. I do not use Fastmail for any vital accounts, since I can spoof emails from them (they have a lax SPF and DMARC record). It was trivial to spoof email to Fastmail because they have limited detection and notification. *See the editor's note at the end for an alternate experience.*

How can we trust any incoming email? All major email providers give you the ability to view incoming email headers, including information added by the mail server and sometimes their spam detection. On most websites/apps there will be a "more options" style button on the email, where you can choose to view the email headers. Clicking on that will give you a ton of extra information about the email.

The things we want to look for in here is where they show DMARC, DKIM, and SPF results. The domain anoni.sh doesn't have any DMARC or DKIM configured, but failed the SPF check. Looking at the header alone (Image 003), you could tell that it's not sent from an authorized server and shouldn't be trusted. This is where another problem comes up as most guides that tell you how to configure SPF tell you to use "~all", or even the less secure "?all". As we've seen it's not terribly hard to spoof an email that's only secured with SPF, especially when we don't have SPF configured in the most secure way.

One reason that I believe "~all" is recommended more than "-all" is that it allows for human error. With "~all" if I were to misconfigure my domain records, or make changes to my mail provider in the future, outgoing email would still be able to reach those I'm sending it to. With "-all" the emails would be dropped, or end up in spam.

What to do with the reports: So you've followed along, got all of your domain records set up, and you're receiving xml files. If you scroll through it, you should see one or more sets of <record> tags that look something like the following compressed data.

```
<record>
<row>
<source_ip>64.147.123.26</source_ip>
<count>1</count>
<policy_evaluated>
<disposition>quarantine</disposition>
<dkim>fail</dkim>
<spf>fail</spf>
</policy_evaluated>
</row>
<identifiers>
<envelope_from>buffer1024.com</envelope_from>
<header_from> buffer1024.com</header_from>
</identifiers>
<auth_results>
<spf>
<domain>buffer1024.com</domain>
<scope>mfrom</scope>
<result>fail</result>
```

We only care about entries where the <policy_evaluated> contains fails. Looking at the <envelope_from> field, we can see someone set "MAIL FROM" to buffer1024.com or a subdomain, and at <header_from> they set the "From" header to something@buffer1024.com.

Our next step is to take the <source_ip> and do a reverse IP lookup on that IP address. You can do it on mxtoolbox at https://mxtoolbox.com/ReverseLookup.aspx. We can see that some criminal using the domain bugs.buffer1024.com is pretending to be us. From here we can report them to their domain registrar, or the IP address to their hosting provider.

What can we do about it? Unfortunately, not much, even if we configure everything perfectly for our own custom domains, all it takes is one mail provider to be lax on scrutinizing incoming email and it may end up being spoofed to their users. DMARC is a big step in the right direction, and most mail providers follow the rules, or at least flag the emails and send them to spam. Most importantly, if you find a flaw that lets you spoof emails to an inbox, report it.

Editor's Note: *After speaking with AmIJesse, I made several changes to my own email settings for all of my custom domains. My addresses are now much less easy to spoof. I am not bulletproof, but I am in better shape. I also now know, through the daily summary emails, that many people try to send spoofed messages in my name. I believe everyone who uses email with a custom domain should apply these settings.*

After applying DMARC to a domain sending email to Fastmail, I noticed Fastmail was completely blocking any messages sent from that domain through a PHP script on my web server. That is the desired action. Therefore, Fastmail does appear to be taking some action to block spoofed messages from a DMARC-protected domain, but not enough to block AmIJesse's advanced attempts. I had to remove the DMARC configuration for that domain to continue my use of that script, which is a good thing. I also like the daily summary from Fastmail easily identifying the number of failed attempts. My opinion is that a DMARC setting on your domain will provide some protection from spoofed messages being sent, even from Fastmail, but nothing is bulletproof. I agree with AmIJesse, email is broken. I hope to have him on the show soon to dive into this deeper.

```
root@bugs:~# telnet smtp.google.com 25   1
Trying 142.250.27.26...
Connected to smtp.google.com.
Escape character is '^]'.
220 mx.google.com ESMTP s15-20020a170906284f00b006ec0ad1e7d2si3354196ejc.286 - gsmtp
HELO localhost   2
250 mx.google.com at your service
MAIL FROM: <admin@google.com>   3
250 2.1.0 OK s15-20020a170906284f00b006ec0ad1e7d2si3354196ejc.286 - gsmtp
RCPT TO: <user@google.com>   4
250 2.1.5 OK s15-20020a170906284f00b006ec0ad1e7d2si3354196ejc.286 - gsmtp
data   5
354  Go ahead s15-20020a170906284f00b006ec0ad1e7d2si3354196ejc.286 - gsmtp
From: <admin@google.com>
To: <user@google.com>      6
Subject:Spoofed Email

Spoofed email   7
.   8
550-5.7.26 Unauthenticated email from google.com is not accepted due to domain's
550-5.7.26 DMARC policy. Please contact the administrator of google.com domain
550-5.7.26 if this was a legitimate mail. Please visit
550-5.7.26  https://support.google.com/mail/answer/2451690 to learn about the
550 5.7.26 DMARC initiative. s15-20020a170906284f00b006ec0ad1e7d2si3354196ejc.286 - gsmtp
quit   9
221 2.0.0 closing connection s15-20020a170906284f00b006ec0ad1e7d2si3354196ejc.286 - gsmtp
Connection closed by foreign host.
root@bugs:~#
```

Image 001

```
root@bugs:~# telnet mail.tutanota.de 25
Trying 81.3.6.162...
Connected to mail.tutanota.de.
Escape character is '^]'.
220 w1.tutanota.de ESMTP Tutanota
HELO bugs.buffer1024.com
250 w1.tutanota.de
MAIL FROM: <spoofedsender@hastysec.dev>
250 2.1.0 Ok
RCPT TO: <amijesse@tutanota.com>
250 2.1.5 Ok
data
354 End data with <CR><LF>.<CR><LF>
From: <spoofedsender@hastysec.dev>
To: <amijesse@tutanota.com>
Subject: This email is not real

This message body could be anything
.
250 2.0.0 Ok: queued as 9E2DEFA0E97
quit
221 2.0.0 Bye
Connection closed by foreign host.
root@bugs:~#
```

Image 002

```
  key-exchange X25519 server-signature RSA-PSS (4096 bits) server-
digest SHA256) (No
 client certificate requested) by mailin012.protonmail.ch
(Postfix) with ESMTPS id
 4KkMn52rqBz9vNPb for <amijesse@buffer1024.com>; Thu, 21 Apr 2022
03:03:37 +0000 (UTC)
Authentication-Results: mailin012.protonmail.ch; dmarc=none
(p=none dis=none)
 header.from=anoni.sh
Authentication-Results: mailin012.protonmail.ch; spf=fail
smtp.mailfrom=anoni.sh
Authentication-Results: mailin012.protonmail.ch; arc=none
smtp.remote-ip=164.92.148.39
Authentication-Results: mailin012.protonmail.ch; dkim=none
To: <amijesse@buffer1024.com>
From: <jessen@anoni.sh>
```

Image 003

AN OSINT BACKDOOR TO UTILITY SEARCHES

By bradm

When you setup new utilities, including things like power, cable, internet, and telephone, your utility company often will provide that data to marketers and data aggregators. This information is valued by private investigators, as utility information can suggest a reliable link between the subject of an investigation and their home address. From an investigator's perspective, access to this data is highly coveted. Services charge as much as $150 to search for a subject through a utility search. By using a common feature in many utility services in an unintended way, we can often obtain enough information to confirm or locate a subject address without fancy paid databases.

Virtually all of the major paid records aggregators purchase and resell access to utilities information, including "live gateway" or "real-time" access. Utility subscriber information provides investigators with the likely current location of target individuals, and is invaluable for people who have recently moved, or those who are more transient and less likely to have a fixed address. Private investigators, skip tracers, bail bondsman, and other investigators prize utility hits for both their "freshness" and their authoritativeness when it comes to establishing a link between a subject and a residence.

Unfortunately, utility subscriber information is often locked away behind expensive databases, many of which will only sell to individuals with particular use cases or industry affiliations. However, many utility companies disclose partial (or complete) subscriber information in response to "outage reporting" functions on their websites. This widely-implemented utility feature is often misconfigured to allow you to search for a utility subscriber by cellphone number. I'm going to focus on electrical utilities here, but much of this applies to other utility providers.

Utility providers often have a "report an outage" feature on their website. Paging through these portals, they will often allow you to input a cellphone number associated with a particular account, and use that cellphone to lookup the subscriber address. The address (or addresses) are then displayed on a subsequent page for users to select the property for which they would like to report a service outage. Usually, the property information is partially redacted, giving rise to a type of information disclosure similar to "account knocking." For example, one major electrical company provides the house number, first two letters of the street name, and the street type. This is often all we need to confirm an active association with the subject and a particular address, using address data obtained through other people search services. Worse, many providers obscure the full address on the client side, transmitting raw JSON data containing the full address (as well as other subscriber details) to the browser. A review of ten major providers uncovered this behavior at two of the ten, one of which is a major publicly-traded company serving much of the United States.

The "outage reporting" information disclosure issue is not isolated to web services. Calls to one very major internet service provider's outage reporting phone number from a subscriber cellphone automatically prompt an automated request to verify that the outage is occurring at a partially-redacted subscriber address. Spoofing the cellphone number of your target and calling these outage lines provides another information disclosure channel which can aid in confirming their location. Some entities allow users to report outages by social security number or tax identification number, in addition to phone number, address, meter number, or account number.

A (very poor) attempt at automating this process was made by the author with a script called outageinfo.py available at https://github.com/outageinfo/outageinfo/blob/master/outageinfo. Readers should note that the script has not been updated in over a year. However, the fundamental information disclosure vulnerability continues to exist in commonly used utility providers across the country.

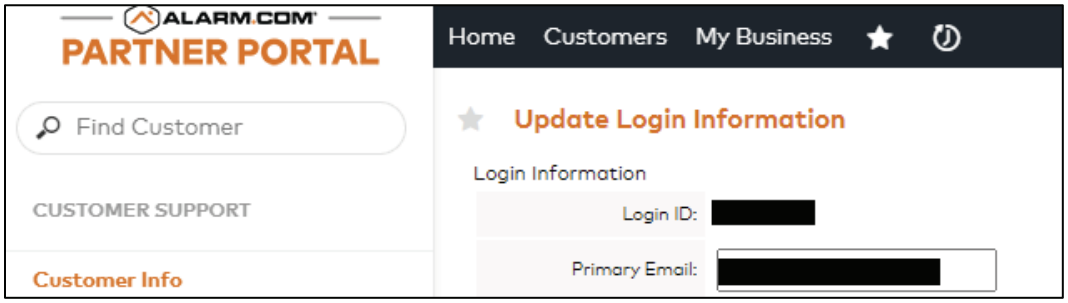
Mitigation: Purchasing utilities in the name of a private limited liability company is likely the best countermeasure against both the sale of utility data, as well as abuses of "outage reporting" functionality. If you are concerned about your exposure to curious parties (ab)using this feature, check if your utilities allow reporting of outages via any unauthenticated method other than service address. Many providers allow for outages to only be reported by service address, or require account owners to login to the site to report outages. Those configurations are likely to protect against the abuse of "outage reporting" portals. Data still may be sold to third parties, however, and made available to commercial search services.

I INSTALLED YOUR ALARM SYSTEM

By Anonymous

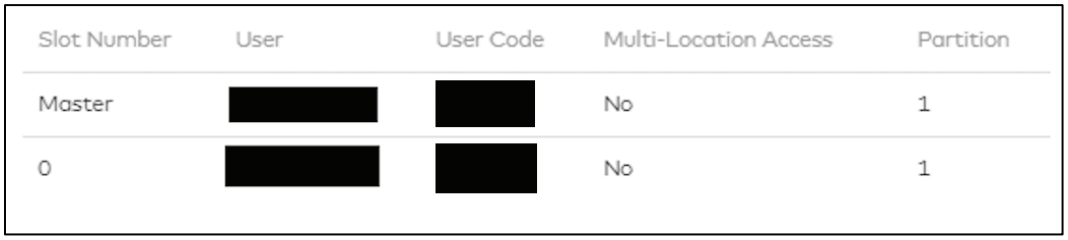
I have been listening to the Privacy, Security, & OSINT show for several years. Michael has warned about the risks of monitored home alarm systems for the privacy purist. His take was that it could compromise your anonymity when the police show up to a false alarm and publicly document your presence. He is right, but that is just the beginning of the potential mess which could jeopardize your privacy and security. You see, I install, configure, and monitor home alarm systems. You may be surprised at what I can see on my end.

One of the most popular alarm systems is by alarm.com. It provides customers a portal where they can log in to see the status of their system, review surveillance video, or make administrative changes. Guess what? I also have access. Each of these systems has an 'INSTALLER' account which I activate during setup. This allows me to remotely monitor your system and make changes if there is a problem. It also lets me do bad things. If you had cameras on that account, I could change your email and grant full access to myself as the installer, then change the email back to the original after my snooping. I can watch everything going on at your house. Here is the screen to grant me access:



The worst part of this is that you receive no notification of my activity. While I am there, I could deactivate your alarm and begin my burglary at your place. If I am not sure about your typical arrival time back to the house, I can load your sensor history and see exact dates and time of alarm activations and deactivations. Here is an example from that screen:

If I am scared to change your alarm code or deactivate it completely, I can just access your codes from the installer portal and use them on site. Here is an example of this screen:



What else can I see? Every system monitored by my company, regardless of the installer. I would never do anything bad with this sensitive information, but other employees of other companies might not have your best interests in mind. Make sure your alarm system cannot be monitored or controlled by strangers. Audible systems are probably enough to deter a criminal. What do I use to protect my house? I have big dogs.

COMMON LAW NAMES AND COVER ID

By Lucky225 (Lucky225@commonlaw.name)

The use of aliases, monikers, nicknames, etc. by privacy, security and OSINT aware individuals for lawful purposes is nothing new, in fact its use predates our current big brother identification regime. However, post 9/11 everyone wants a photo ID to prove the use of the name you're currently going by. In this article I'm going to explain how to lawfully obtain photo ID in a name of your choosing for Cover ID use in the USA. First, of course, I must provide the usual disclaimer, I am not an attorney and nothing in this article is legal advice, you should seek the advice of a local attorney to see if any method described here conflicts with local law or regulation in your particular jurisdiction.

At common law, which all of the original States adopted (and at least 44 States still follow today) via reception statutes and/or case law, one has a right to and can adopt a new name simply be declaring the new name and using it, so long as there is no fraudulent intent. Exceptions to this common law right are Oklahoma & Maine, where the courts have ruled court-ordered name change statutes abrogate the common law which is out of accord with the majority of the US States that say these statutes are IN AID of the common law, and simply provide an ADDITIONAL method to make the change; Illinois where the legislature abrogated the common law right by statute in 2010; Louisiana which was always based on French civil law and never inherited the common law; and possibly Hawaii as there isn't enough case law on the issue and they had adopted their name change statutes prior to becoming a US territory and Statehood.

Outside of the previously mentioned exceptions, the concept of a "legal name" in this country is one that is a shared delusion. In fact, as far as Federal and most State law is concerned, there is no such thing as a legal name. The use of an alias, in most cases, is one's 'legal name'. The use of a name other than the one that appears on your identification, for most purposes, is entirely legal, for example you can enter into contracts in any assumed name you want and you will be legally bound to the performance of the contract.

Of course, in today's world where everyone wants identification to prove you're you, this right is of little help in practice if one cannot obtain identification in the desired name. It's also of little help if one cannot simultaneously possess 2 or more identification credentials in multiple names at the same time. Thankfully, despite what most people believe, this isn't the case. There are various ways to obtain identification in a new assumed name.

The easiest method is to assume a new name on a US Passport. Thanks to case law from 1979, this is completely legal and it's codified in the CFR's as well as the State Department's policy.

United States v. Cox, 593 F. 2d 46 states:

The second rule is that statutes are to be interpreted with reference to the common law and where there is no indication to the contrary, given their common law meaning. United States v. Monasterski, 567 F.2d 677, 681-82 (6th Cir. 1977). Applying these principles to section 1542 we conclude that it is not violated by one who lists a legally adopted name on a passport application. The term "false statement," strictly construed, cannot be held to include use of a legally adopted name. Under the common law a person may freely change his or her name without any legal formalities. Thus, application of both rules of statutory construction leads to the conclusion that there was no evidence that the defendant made a false statement on his passport application.

22 CFR § 51.25 states:

(c) A name change will be recognized for purposes of issuing a passport if the name change occurs in one of the following ways.
(4) Operation of state law. An applicant must present operative government-issued legal documentation declaring the name change or issued in the new name.
(5) Customary usage. An applicant who has adopted a new name other than as prescribed in paragraphs (c)(1) through (4) of this section must submit evidence of public and exclusive use of the adopted name for a long period of time, in general five years, as prescribed in guidance issued by the Department. The evidence must include three or more public documents, including one government-issued identification with photograph and other acceptable public documents prescribed by the Department.

8 FAM 403.1-4(E) states:

a. The Department recognizes a less formal method of name change through customary usage over a period of at least five years (22 CFR 51.25(c)(5)).
b. An applicant may only request a change of name by customary usage on form DS-11.
c. The applicant should present three or more public or private documents, including one government-issued ID with photograph, reflecting exclusive use of the acquired name, each one evidencing that they have used the assumed name for five years or longer. The applicant may not be able to submit an acceptable ID because many issuing authorities do not issue IDs that are valid for five years or longer, and because many issuing authorities retain expired IDs. If this is the case, you may accept the applicant's currently valid ID and two additional documents that meet these criteria.
d. If the assumed name has not been used for five years, or if the documentation provided by the applicant does not show exclusive use, i.e., the applicant has used the former name at any point in the last five years, the applicant cannot change their name by customary usage. The assumed name may still be included as a "known as" name (see 8 FAM 403.1-6).
e. The documentary evidence must show the issue date, acquired name, and one other piece of identifying data such as the applicant's date of birth, place of birth, age, photograph, or Social Security number. Acceptable documentary evidence includes, but is not limited to:

(1) Driver's licenses;
(2) Non-driver state-issued IDs;
(3) Military records;
(4) Employment records;
(5) Tax records;
(6) School records;
(7) Census record;
(8) Medical RECORDS; or
(9) Religious records.

f. Form DS-60, "Affidavit Regarding Change of Name," or equivalent notarized affidavits, executed by two or more persons attesting that they have known the applicant by both the original and assumed names, and that the applicant has used that name for all purposes for at least five years, may be provided in place of one of the public documents if the applicant cannot obtain a third public record. See 8 FAM 401.5 for further guidance on identifying witnesses.

NOTE: Both parents must provide notarized written consent in the assumed name for minor applicants, i.e., the form DS-3053 must list the minor's assumed name (see 8 FAM 403.1-4 for more information on notarized written consent).

EXCEPTION: The general policy in 8 FAM 403.1-2, that all documents must be original or certified copies, does not apply to valid IDs submitted in response to an IRL, as the applicant may need to retain those during the application process. Photocopies of valid IDs are acceptable.

The TL;DR is that you can get a passport in an assumed name, or at the very least get your assumed name listed as an AKA in the back of the passport (see 8 FAM 403.1-6 "KNOWN AS" AND PROFESSIONAL NAMES), I did this myself by first obtaining a Selective Service registration card in the new name by sending a letter to them informing them I had changed my name at common law, then I used that card as an I9 document to update my payroll at work, so then I had pay stubs and health insurance cards in the new name and that along with some affidavits from people that know me was enough to update my passport with a 'known as' name. Using my updated Passport alone, I applied for Global Entry (https://globalentry.gov) and obtained a Global Entry ID card in the newly assumed name, this identification is invaluable as it has name and date of birth and lets you cross into Mexico and Canada using only the Global Entry card as identification alone.

Alternatively if you don't want to go through all that hassle, you can obtain Massachusetts State ID in any name you want. They will have to verify your current name, SSN and DOB match up with Social Security, but after that they can issue you a new ID in any assumed name per their policy - AND you can obtain this ID even if you are not a Massachusetts resident as they have a form of State issued ID called "Liquor ID". This ID card is for out of state residents as their liquor ID laws don't recognize out of state ID as valid, only Massachusetts ID, Passports and US military ID are valid defenses for accidentally serving underage individuals alcohol. As a result, Massachusetts has this weird exception to the rest of the States where out of state residents can obtain State issued ID, and since they follow the common law they will also issue ID in any name you want. See https://www.mass.gov/how-to/change-information-on-your-drivers-license-or-id-card which states:

If you are applying for a Standard driver's license or ID card, you may change your name with no documentation as long as there is no attempt to defraud.

The only downside is Massachusetts will not renew Liquor IDs so you will have to fly back there every 5 years if you are not in close proximity to the state. However, since the Liquor ID is not "Federal Real ID compliant" possessing it with other identification like your driver's license is usually legal (at least Federally, check your State and local laws about possession of out of state ID, most States only make it a crime to possess multiple driver licenses since they give you the privilege to operate a motor vehicle). Of particular note, Massachusetts case law also makes clear using multiple names is legal - "*Where a person is in fact known by two names, either one can be used. This principle has been applied in about every connection.*" Young v. Jewell, 201 Mass. 385 , 386 (1909)

Once you have amassed this identification, it's easy to build on, I was applying for a transportation industry related job recently and they wanted me to get a TWIC credential, checking their website it said a Global Entry ID alone was valid to obtain a TWIC, so I applied for it in my Cover ID name. When I arrived they said Global Entry would not suffice, however I pushed them and showed them their own policy from TSA's website and they eventually relented and issued me a TWIC in the alias name.

Most of us privacy minded individuals will probably be using our Cover ID for hotels and transportation and if that is your use case I highly recommend Global Entry and TWIC if you qualify, both come with TSA pre check and you can fly in your alias name with them alone and I haven't ran into any issues checking into hotels with them.

If you would like to learn more about common law name usage, I suggest checking out my site I built for it at https://commonlaw.name, where I have compiled State-by-State case law and other common law name specific information as well as more details on US Passport information, and even getting an Amateur Radio license under an assumed common law name, with links to legal papers discussing this topic.

Editor's Note: *I agree with Lucky225 that you should never take anything in this magazine as legal advice, but the content here is very interesting. I plan to research more and attempt execution of an alias Massachusetts Liquor ID card. If I do so without incarceration, I will post an update.*

SUCCESSES AND FAILURES OF A PRIVACY ENTHUSIAST IN A NON-ENTHUSIASTIC FAMILY

By Oyzark

I am a privacy, security and technology enthusiast, most happy when tinkering with and trying new technologies. For me, it is truly a hobby - I love to explore what is possible and push what can be done with technology. I have a spouse for whom technology is a necessary and relatively uninteresting means to an end, and four teenage kids. One shares an interest in privacy and security, and she is motivated to try new strategies and tools. The other three are firmly in the "means to an end" camp. Below I share some of my successes, partial successes and failures in attempting to implement family-wide privacy and security measures. The successes all share something in common - they provide some significant benefit beyond privacy and security to the family, with minimal cost. The failures usually stem from me incorrectly projecting my geeky enthusiasm onto the family. At the end I give some overall lessons I have learned which I share in the hope they are useful for others in a similar situation.

The successes

A whole house pfSense router/firewall with VPN: We have a modest sized house that is just a little too big for good coverage with a single Wi-Fi router. A couple of years ago I decided to replace three separate routers (and three separate Wi-Fi networks) with a pfSense router/firewall with three professional UniFi hotspots. The beauty of using the UniFi hotspots is I could set up multiple Wi-Fi networks that are broadcast on all the hotspots, with each network corresponding to a different virtual network (VLAN). One VLAN passes through ProtonVPN (used mainly by me); one is open (used mainly by family); and one is for devices. pfSense lets me have lots of control over the security of network as a whole, without any negative impact on the family. This change was a big improvement for the family - Wi-Fi is simpler and has better coverage, speed and reliability. Meanwhile I get the whole house VPN and a chance to do security tweaks!

Secure messaging: This one was relatively easy, as the family was already naturally migrating to messenger apps, just the ones we don't like (WhatsApp, Instagram and Facebook Messenger). After setting up a family Signal group it took a couple months of off and on usage before everyone defaulted to Signal as a primary family communications method. A success which I nearly blew a few months later when I decided to move the family group to Wire, as I wanted to be able to use more than one device for my account. After many sighs and eye rolls, the family made the move, and we now keep Signal as a backup and for non-family messaging. This actually worked out quite well in the end, as Wire is only used for immediate family communications. We know that if we get a message on Wire it is a "priority family" message versus the background noise of other notifications.

Prepaid cellphones: This was an easy win, as prepaid plans are considerably cheaper than postpaid, and concerns about being billed wrongly at the end of the month and being tied to a carrier go away. My spouse and two of my kids still use their "real" cellphone number, but at least it is in a prepaid plan in a generic name. We ended up putting all the family cellphones onto one account that everyone can access which makes management easier than having separate accounts for each plan (albeit at a slight cost to privacy). Interestingly, my youngest two kids see no use for a cellphone number anyway and always use messengers.

Internet data removal: Using the free IntelTechniques workbook, it was relatively easy for me to, with permission, go through the removal process for my spouse at the same time as for me. Even non-enthusiasts have some concerns about having their information on the Internet, and my spouse was happy to have someone do some cleaning on her behalf.

The partial successes

Use of a home alias: It actually surprises me that this one worked at all. It began when I started using an alias name for delivery of Amazon packages, and it kind of spread from there. Family members would laugh at me getting packages in a slightly goofy alias name. I then set up an alias for my spouse and she started receiving Amazon packages in an alias name. With a companion MySudo phone number and ProtonMail address, my alias is fleshed

out enough to use for food deliveries and other online orders. Our home aliases are not really very robust, but by making it a goofy, fun thing we are normalizing the idea that you don't have to use your "real name" for many things, while reducing the amount of companies that have our real name and home address together on file.

Use of a PO Box for mail: I got somewhat lucky on this one, as we moved house a few years ago and it was natural to use a PO Box for mail in the transition, and we just kept it going. I take on the burden of fetching the mail weekly, and at least a moderate amount of mail (and most of the junk mail) now goes to the PO Box (actually the street address of the post office) instead of our home address. However, the benefits to the family are not very clear, and it creates some hassles - for instance our bank uses the PO Box, which has a different ZIP code to our home address, so family members have to remember another ZIP code for using the credit card at the gas station. Overall I have gotten away with this one, but the family isn't too happy.

Password managers: I really tried to get everyone using password managers. Of course, my privacy-loving daughter uses one, and one of the other kids uses one just so he doesn't have to remember passwords. For the others, using a password manager is apparently just too clunky. We have had to resort to printing out account information, and using somewhat complex, unique but memorizable passwords for some shared accounts.

Masked credit cards: The family was dubious about this one until we got into one of those regular situations where we tried to cancel a magazine subscription, but they still kept billing us. Because we had used a Privacy.com masked credit card we could simply delete that card and we never had to worry about it again. Using Privacy.com is still rather clunky for some family members and we're not using it universally, but overall it's been accepted and beneficial.

Unique email addresses: I have a domain set up at GoDaddy where individual addresses can be forwarded to different accounts. This works very nicely for having unique addresses for each service that can forward to more than one person - for example, we can have amazon@mydomain.com which forwards to both me and my spouse. This is working and has been accepted by family members, but it fails the "significant benefit" test and remembering which email is used for what is an added complication for people.

NextCloud home file server: I have an Ubuntu box on my home network that is set up as a NextCloud server. This is perfect for me, as it lets me synchronize files and photos across devices as well as providing a single repository that can be backed up easily. It also solves the difficult problem of sharing photos among family without having to get entangled with iCloud and its ilk (my phone and my spouse's phone automatically upload photos to a shared folder on NextCloud when on home Wi-Fi). The NextCloud app is not super slick, but does allow access to files and photos when necessary. It's not a perfect solution and several family members are also using iCloud, but at least it's some progress.

The failures

VoIP: I love my pack of nine MySudo numbers, but VoIP just didn't work for family members. Three of them already had a number they were attached to, and didn't want to risk porting it to VoIP along with having to learn a completely new app for texting and phone calls, and confusion about reliability and where and when you can call 911. The other two, as previously described, don't give out phone numbers anyway. This has been mitigated somewhat by us porting our old landline to Google Voice, which can then be forwarded to cellphones. Thus family members often give out this number rather than their cellphone numbers. Another VoIP mess came from me changing my phone numbers regularly and them never knowing which is the "real" one (tip: have one VoIP number for family and don't change it).

DeGoogling: I have pretty much entirely removed Google from my personal life (still need it for work), but Google is so pervasive I have to accept others in the family will use it. All of them use Gmail as their primary email (I keep a legacy Google account but don't really use it), and much schoolwork gets done using Google Docs and Chromebooks. I don't feel too bad about this, as at least Google is secure even if it's not private.

Keeping our home address completely private: The PO Box and the use of a home alias have really helped keep our home address off the popular people search websites, but keeping our home address completely private is too much of a leap given our family situation. It only takes a small leak in a water pipe to flood the basement, and similarly it only takes a few places to know your home address for a flood of junk mail to arrive. The school district requires declaration of a physical residential address to prove your kids are eligible, but once they have it you have lost

control. Beware the college board. Recently one of our kids took an SAT test, which required registration with the college board, including automatic population of home address from the school district records. We now get 3-4 pieces of junk mail a week to his name at our home address. Even without this, it is just too much to expect all the family members to use alias names all the time.

General lessons

Of course, every family situation is different, but here are some general lessons I have learned.

Keep your privacy hobby compartmentalized. Don't try to drag your unwilling family into your extreme privacy escapades! Have your own sandbox where you can play without affecting the daily life of your family.

Use a realistic threat model for your family. As a privacy hobbyist, I am constantly imagining advanced threat models. I am fortunate that I am not being hunted down by a violent ex-spouse, I am not a journalist or whistleblower, and I am not trying to flee a repressive country. But I love imagining what I would do if I were, and trying out the technologies I would use in various extreme scenarios. This can sometimes make it hard to keep your family threat model realistic. Your family threat model should likely be about the simple things that get most people like phishing attacks, device failures and account compromise.

Only implement measures that benefit everyone. Before suggesting a potentially disruptive change to family protocol, make sure you can clearly explain the real benefits to them, as well as the cost. The explainable benefits should far outweigh the costs.

Don't hide things from your family. You probably think it's normal to have fifteen ProtonMail accounts and nine phone numbers, but your spouse might not think it is normal, and if you are constantly doing mysterious things in your basement your family is going to think it's a little weird. Make sure you are not hiding things from your family and especially your spouse, otherwise it can raise suspicions, and your relationship needs to be based on trust. Explain you enjoy this exploratory hobby, and offer to walk your spouse through your privacy setup (of course this does not apply if you are in an abusive relationship and needing to exit). Be content with improvement rather than perfection. Celebrate the wins!

Editor's Note: *I really like hearing about other people's experiences with the privacy game. This helps all of us. I hope more people submit their own successes and failures.*

OSINT CORNER

By Jason Edison

Jason instructs live and online open source intelligence courses for IntelTechniques in addition to working as a cyber-crime detective for a large US police department. Each issue will feature an OSINT tactic from the IntelTechniques online training.

One of the aspects of working in open source intelligence which I enjoy the most is that every day I discover something new. Often new techniques are incredibly simple and yet can greatly improve the efficiency and/or quality of our intelligence work. These discoveries almost always come from discussions and collaborations with colleagues from our community. One such technique came up as I was talking through a recent browser lesson with Michael. He explained the use of what I like to call a "hard page refresh" in Chrome and Firefox. This the process of forcing a web page to fetch the most recent page assets, such as images and other media.

Why might we need to force a page to reload all assets? Sometimes when visiting pages, certain objects and files may be cached despite there being an updated version on the web server. So, the results we initially see may change if we force the page to ignore the cached files and reload all files entirely. Now, in some instances seeing yesterday's page assets today may benefit us, for example, if we are looking for deleted content. Still, we are often seeking out the most current intelligence, and it may be helpful to know how to force the page to display the most recent content changes.

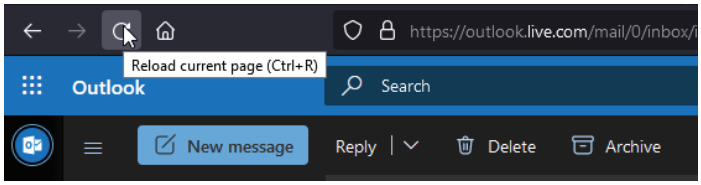
Imagine a scenario where you are collecting not only intelligence, but also capturing pages as evidence for a criminal or civil investigation. You could face unnecessary evidentiary challenges in court if the opposition is able to show that your page captures did not actually include the most recent images and other assets on the day that you preserved them. In fact, a question you could face on the stand is: "as an investigator how can you be certain that the web page you submitted to evidence was truly from the date and time in question?" A good best practice when preserving a key piece of online evidence is to capture the initial page, then force the site to reload the page assets, and then capture the page a second time for comparison. Many times, there will be no difference, but what you will find is that occasionally the page will have changed after that hard refresh.

This tactic of forcing a hard page reload is even more important if you are preserving metadata with your page captures. For example, when using SingleFile or Hunchly to capture pages at the code level, along with digital assets, we want to make sure that we've loaded the most recent images and other media. Otherwise, file timestamps and other metadata will likely make it painfully obvious that we failed to preserve the most recent and accurate page content.

How we force this hard refresh could not be simpler and being a fan of hot-keys for efficiency, here are your key combinations for Firefox and Chrome on Mac and Windows/Linux workstations:

Firefox: CMD-Shift-R / CTRL-Shift-R
Chrome: CMD-Shift-R / CTRL F5

As with all techniques there are pages and situations for which the standard hot-keys will not function as intended. For example, on some pages such as forums or webmail, hitting CTRL-Shift-R may initiate a reply to the currently selected message rather than reloading the page assets. If you run into one of these difficult pages, where the hotkeys do not function as expected, we can force the page to reload assets another way by holding down *Shift* and clicking on the page refresh icon on the address bar:



It is always important to have multiple methods of initiating any OSINT technique and some of you may even prefer shift-clicking the reload icon over using just hotkeys. You can find many similar techniques by joining the IntelTechniques online training at IntelTechniques.net.

INTERCEPTING VEHICLE MAINTENANCE VIDEOS

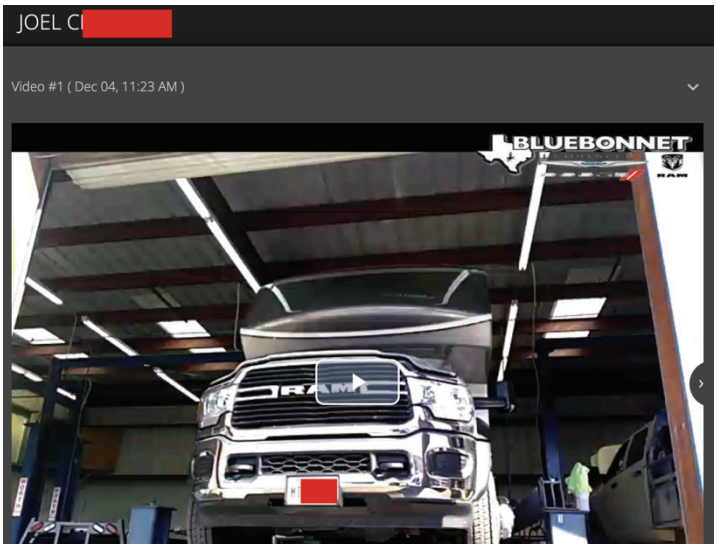
By Michael Bazzell

I debated whether this article should be included in this magazine. Some will read it and think this privacy violation is no big deal while others might see it as an investigation strategy. I present it as neither. I will simply outline my experience as an educational opportunity, and allow you to digest it as you wish. This all began last week when a family member shared something interesting. He had his vehicle serviced by a dealership and received a video of his car problems via email. The video was to visually display the issues which were found, likely in an effort to convince him to pay for the optional repairs. I will not expose this family member's video, but we will take a look at other videos which are publicly available.

Let's conduct a Google search for the exact phrase "app.truvideo.com/v/" within quotes. The result is over 100 websites where people have publicly shared their own maintenance videos to the world, hosted by TruVideo. The first Google link is to a vehicle forum which contains the following link to a video.

https://app.truvideo.com/v/coHMYT

Clicking this link presents a page with an embedded video, the name of the vehicle owner, dealership information, and full license plate, as seen below (redacted).



Playing the video audibly confirms the customer name and allows us to see the inspection of the vehicle and needed repairs. Now, what is the big deal? If no one knows the link to your video, they cannot see the details. The videos appear to have a randomly generated six-character URL title. Would anyone find YOUR video? Probably not, at least not like this. Let's keep going.

When you play the video and copy the video link, you will see it navigates to the following URL.

https://tce-in.s3-accelerate.amazonaws.com/ee72d81148aac6fc6c81654ffcaba79.mp4?t=1651244561228

This video is hosted within an Amazon AWS bucket titled "tce-in". If you navigate to the following link, you will see 1,000 records of videos within other embedded pages.

http://tce-in.s3-accelerate.amazonaws.com/

A random record has a "Key" of 0004BC29-504D-4A80-A044-02B7CC2B0729.mp4. Therefore, the following URL should display that video.

http://tce-in.s3-accelerate.amazonaws.com/0004BC29-504D-4A80-A044-02B7CC2B0729.mp4

I can now watch random videos of strangers' vehicle issues. If 1,000 videos is not enough for me, I can use the following links to display all videos by key in alphabetical order. Inserting numbers instead of letters finds more. Since this app also uses a bucket called "tvin", I can replicate my queries as listed below to identify several thousand videos.

http://tce-in.s3-accelerate.amazonaws.com/?marker=A
http://tce-in.s3-accelerate.amazonaws.com/?marker=B
http://tce-in.s3-accelerate.amazonaws.com/?marker=C
http://tvin.s3-accelerate.amazonaws.com/?marker=A
http://tvin.s3-accelerate.amazonaws.com/?marker=B
http://tvin.s3-accelerate.amazonaws.com/?marker=C

This was all fun, but I never natively found my relative's vehicle. I returned to the URL of his video page and looked at the source code. I found the following entry, which I redacted:

```
<meta property="og:title" content="376xxx"/>
```

The last digits appeared to be his customer number or order number, as they were unique for every video. I called the dealership which was present within the logo on the back of his vehicle and stated the following.

"Hi, I am trying to add a bill to our fleet records, but I am not sure which vehicle it belongs to, if I give you an order number, can you look it up? It is 376xxx".

The person responded with the full details of the customer, including name, address, and vehicle information. Again, I am still cheating since I had already been given video URL, so I asked my relative for a copy of the receipt. Sure enough, that order number was visible. Unfortunately, a search for it did not connect me to the video. I would need to brute-force scrape all of the pages (based on the six-digit identifier of each) in order to truly get what I needed. I did not do that because I didn't care enough. I suspect someone will soon.

I wanted to see the full entry for my relative's video, so I navigated to a URL of "http://tvin.s3-accelerate.amazonaws .com/?marker=" followed by the file name of his video without the mp4 extension. A random example shown below would have been the following URL:

http://tce-in.s3-accelerate.amazonaws.com/?marker= 7956102fa5321e7aa030eec4ad72c8a8.mp4

This displayed over 1000 videos beginning with my relatives unique entry, including "<LastModified>2022-04-25T15:27:55.000Z". I now know that this vehicle inspection occurred on April 25 at 3:27 pm (in an unknown time zone). The source code of the original video page displayed the following line, which I redacted for privacy:

https://tce-in.s3.amazonaws.com/THUMB/ 51..._mp4_thumb.png

This linked to the thumbnail used when initially loading the video page. I could scrape all thumbnails based on the Amazon bucket quite easily. Most of them display a license plate in order to prove to the customer they are watching their own vehicle. Text recognition software could generate a list of plates, but I can't think of why I would want that.

Does any of this help me? Not really. Is this an invasion of privacy? I don't know. My relative did not recall signing any consent form to upload video of his vehicle, but he also wasn't looking for such information. Is this a powerful OSINT tip? I don't think so. However, consider this for the next time you encounter something more valuable which connects to an Amazon bucket. These techniques may have more value then. This article may lead you on your own journey investigating services which use open Amazon buckets and the details which can be easily gleaned. Please be kind when you find anything sensitive.

```
−<ListBucketResult>
    <Name>tce-in</Name>
    <Prefix/>
    <Marker>7956102fa5321e7aa030eec4ad72c8a8</Marker>
    <MaxKeys>1000</MaxKeys>
    <IsTruncated>true</IsTruncated>
  −<Contents>
      <Key>7956102fa5321e7aa030eec4ad72c8a8.mp4</Key>
      <LastModified>2021-06-07T19:26:12.000Z</LastModified>
      <ETag>"61fc57dd1b06ddac85d7294d80419524-11"</ETag>
      <Size>55097420</Size>
      <StorageClass>STANDARD_IA</StorageClass>
    </Contents>
```

NEW GOOGLE CONTENT REMOVAL OPTIONS

By UNREDACTED Staff

As we were finalizing this issue for publication, Google announced a policy change in their offer to "Request the removal of personally identifiable information that appears in Google Search". This went viral online and caused many people to celebrate this new ability to finally remove sensitive information from Google's search. Oh, if it were only that easy. Yes, they did add additional types of information which can be removed, but it is not going to help people immediately hide all online sensitive details. Let's take a look.

For many years, people have been able to force Google to remove signatures, bank account numbers, and other details which could lead to identity theft. This has been a staple of the services which we provide, and we have used this policy in the past to help our clients. This week, Google stated in an official blog post that:

Under this new policy expansion, people can now request removals of additional types of information when they find it in Search results, including personal contact information like a phone number, email address, or physical address. The policy also allows for the removal of additional information that may pose a risk for identity theft, such as confidential log-in credentials, when it appears in Search results.

This sounds great, and we might be able to benefit from this. However, as you look closer, you will find the following requirements for this luxury:

For us to consider the content for removal, it must pertain to the following types of information:

- *Confidential government identification (ID) numbers like U.S. Social Security Number [...]*
- *Bank account numbers / credit card numbers*
- *Images of handwritten signatures*
- *Images of ID docs*
- *Highly personal, restricted, and official records, like medical records*
- *Personal contact info (physical addresses, phone numbers, and email addresses)*
- *Confidential login credentials*

For us to consider the content for removal, it must meet both of these requirements:

- *Your contact info is present.*
- *There's the presence of explicit or implicit threats, or explicit or implicit calls to action for others to harm or harass.*

In summary, you have always been able to remove copies of ID, signatures, or bank account numbers from Google's search algorithm. This new policy adds two new features. The first is the ability to remove full contact information (address, phone, email). This sounds amazing and would be very helpful. However, there is a catch. From Google:

When we receive removal requests, we will evaluate all content on the web page to ensure that we're not limiting the availability of other information that is broadly useful, for instance in news articles. We'll also evaluate if the content appears as part of the public record on the sites of government or official sources. In such cases, we won't make removals.

In other words, if your contact details are present within any form of "news" website, including blogs, or if your home address was scraped from an official county source, your information will NOT be removed. The new doxxing removal option has two requirements, both of which must be met. First, your contact information, such as your home address, must be visible, AND there must be an implicit threat to harm or harass you. In other words, presence of your details and a negative comment about you does not meet the requirement.

This seems like virtue signaling from Google. Only in very few cases of legitimate threats will the information *possibly* be removed. As we write this, numerous people are posting their content removal rejection letters from Google. While you might force their hand on some contact information removal, they will never remove the content which traces back to an official source. People search websites will still possess all data which *might* be removed from Google as a link. This is why we always recommend keeping your true information off of government websites, such as titling your home and utilities within a trust or LLC.

LEAVING KINDLE FOR BOOX

Product Review by Michael Bazzell

I have been very vocal about my issues with Amazon's Kindle e-book reader. Each Kindle collects and transmits a lot of data as you quietly read your books. Amazon eagerly records all books which you have purchased through the device, all books which you have read through the device, all books which you have searched from the device, the last page read of any book in your account, any annotations, highlights, or markings within all your books, the speed at which you read, your language settings, all Wi-Fi and Bluetooth connections, your estimated location and signal strength, and the times and dates of usage within device log files. All of this is neatly noted within your Amazon account, which is required to use the device. If Amazon removes a book from their service, they remove it from your device too. No thanks.

In my book Extreme Privacy, I discuss ways to prevent this data transmission, but it requires you to never connect your device to any internet connection, which limits your book loading abilities. My other main complaint about Kindles is that they rely on a closed proprietary operating system which gives us no control of our usage and data. You can't take advantage of their E Ink system with loads of free online content. Kindle wants you to never leave their premium ($) ecosystem. For many years, I played the game with them. I have used programs such as Calibre to scrape news websites and load data to the device, but I am tired of the hassle. This year, I decided to put the Kindle down and find better alternatives which would give me full access to all features available in a standard tablet while still presenting the content within E Ink, which is much better for eye fatigue.

I started with a Kobo e-reader, which was disappointing. There was significant lag and the entire experience was underwhelming. I then tried the Onyx BOOX readers, and realized that I have been missing so much for the last several years. I have since used both the 10.3" Note Air2 and the larger 13.3" Max Lumi2. I wanted a large reader because the majority of the content I ingest is within a standard PDF format (such as this magazine).

Let's pause and talk about format. Readers such as the Kindle require books which have been formatted into a scrolling feed which can be read on various sizes of devices. This works great for novels, but is awful for textbooks and large technical books. If you have ever tried to convert a PDF to MOBI for Kindle, you know the pain which this creates. I want to read books exactly how they were printed. As an author of technical books, I know how important layout is to the experience. I want the pages to flow in a specific way and images to appear as they would in a print book. I want my fonts to be replicated to the reader and not switched to a single standard font throughout the book. Reading in PDF preserves all layout. However, opening a traditional PDF within Kindle results in text too small to read. This is where BOOX devices excel.

I started with the Note Air2 with the 10.3" screen. PDFs looked great and page turns were smooth. I could finally read a PDF as it was intended. I buy a lot of Humble Bundle book deals and also purchase digital versions directly through sites such as No Starch Press. I could now open all of the native PDFs on a large screen reader and digest the books as the author intended. This was a huge deal to me. I could also load and remove books easily from my computer without Amazon creeping on my activity. I felt in control. I also felt it in the wallet. These large screen devices range from $475-$899 USD.

Next, I was excited to really take advantage of these new readers. I tried the 13.3" Lumi2 which provided a true 8.5" x 11" screen which allowed me to view US paper-sized PDFs without any scaling. This was another bonus. I like to read newspapers from three cities spread over the US. This eliminates the option of local paper delivery, so I rely on my digital subscriptions. One paper I read often is the Wall Street Journal. For several years, I have used Calibre to scrape the articles and transmit them to my Kindle via USB cable. The experience was "ok" since I had a digital subscription, but I constantly received partial articles or missing sections. It was enough to almost get the job done, but not very enjoyable. The WSJ offers a full PDF of each day's issue, but reading that on a small screen was impossible.

I loaded the full paper PDF in the Lumi2 (in horizontal mode), and read the paper cover-to-cover as it was intended. The layout was identical to the print version, and the font was an appropriate size. THIS was how I wanted to get my news every morning. I was done staring at a monitor or scraping partial data.

I am embarrassed to report that it took me a while to realize I could just do everything on the device itself. With embedded Wi-Fi which does not send data back to Amazon about my usage, I could browse the web, download news, and retrieve my full daily PDFs from each source. I no longer need to connect it to my computer.

BOOX's devices rely on a very minimal version of Android 11 as the operating system. After using ADB to disable any undesired apps, as explained in Extreme Privacy, there were no unnecessary Google or Onyx apps calling home. I had expected a need to remove more invasive apps but was pleasantly surprised when none appeared. I installed F-Droid and Aurora Store, as I explain in my book, which allowed me to download apps without a Google account. I could have downloaded my email app, but that seemed contradictory to my desire with this device. Connecting it to my computer via USB cable immediately allowed me to work with the device through Calibre. I transferred my stored e-books from there, and both MOBI and EPUB versions displayed great on the device. Again, something you cannot do with a Kindle which requires MOBI or AZW.

We should discuss book purchases. Kindle has an easy way to browse and purchase books directly on the device. While convenient, we have the same problems presented at the beginning of this article. With BOOX readers, you can load anything you want from any system. When I want to purchase an e-book, I go straight to the author or publisher. Most sell direct now and include access to a true PDF copy. If you have a ton of Kindle books which you don't want to lose, you could install the Kindle app on these devices and have the best of that world. If you follow my book and use NextDNS to act as a firewall, you can block all outgoing Amazon connections after the account is connected.

Many older books are completely free at Project Gutenberg and Archive.org's Open Library. Your library likely offers an e-book lending option which should work on any Android device. Mine offers unlimited e-book borrowing and a huge catalog. You don't NEED Amazon. I don't even need to physically visit the library to check out free e-books.

BOOX devices were designed for people who want to read a book minutes after turning it on, and not for geeks like me. There are a few tweaks I made in order to possess a more robust device. First, I updated the system firmware with the embedded app, which only took a few minutes. I then customized the "Navigation Ball" feature which places a small circle anywhere you want with quick menu items. This allowed me to easily get to my library or refresh the screen. Since I read mostly during the day in good lighting, I disabled the backlight features and E Ink enhancements (just my personal preference). Finally, I installed Firefox via Aurora, added the uBlock Origin add-on, and installed Blokada to block any remaining undesired connections.

It took me a while to take advantage of their magnetic "pen" which allows me to annotate directly within files, take notes, or doodle. I don't do any of this often, but I have read extremely technical books and benefited from the ability to circle areas which I would need to revisit. I plan to take advantage of this more in the future.

It seems unfair to keep calling these things e-readers. They are really full-functioning Android tablets which are easy on the eyes with a week-long battery. Today, my mornings start with my Lumi2 reader. I have my three newspapers (and subscriptions) saved within the device which allows me to pull down that day's print PDF in a few minutes. The E Ink has a look of a real newspaper and I don't experience eye fatigue. I can read outside in full sun and not receive a glare or washed-out screen. My evenings consist of either a tech book PDF or a traditional EPUB biography.

The 128GB storage allows me to carry everything with me at all times, even the entire Mad Magazine archive I found on DVD, including the issues I read in the 80's (this seems to be too much information). Since putting down the Kindle and adopting a large-screen reader, I have found numerous magazine subscriptions which are available in native PDF. I can never go back to the Kindle now.

If you have no need for the larger screens, or your budget prevents this luxury purchase, their standard 6" readers start at under $200, and look better than most Kindles. Full details are at **https://shop.boox.com**. This is NOT an affiliate link and BOOX did NOT pay me for this review. The image on the following page displays my devices with active content (and banana for size).

E-readers and E Ink are nothing new. However, the BOOX devices allow us to leave the small Kindle ecosystem and explore more capabilities without harsh digital screens. After playing with these devices for a few days, my Kindle felt like a single-use tool which limited me from taking advantage of the technology within the unit. I now have full control of my device and my content. I also don't have Amazon snooping on me. You can hear my full review in episode 259 of my podcast.

The Onyx BOOX 10.3" Note Air2 (left) and the larger 13.3" Max Lumi2 (right) with case and pen.

Reader Q&A

By UNREDACTED Staff

Do you have a question or need clarification about a privacy-related topic? Submit it to us for publication consideration at UNREDACTEDmagazine.com. If you have questions, other people are wondering the same thing! Please make sure your submissions are actual questions, and not vague statements with a "?" at the end. Here are questions from last month.

Q: What is the best secure "Dumb Phone"?

A: Any true "Dumb Phone" would probably suffice. We like minimal flip phones without any operating system which allows apps. Our preference is a cheap phone which can be considered disposable. We typically only use these temporarily for clients who need one for emergencies. We buy them with cash at local grocery stores for less than $40. If you wanted something long-term, check out the Light Phone or Punkt devices. Both are overpriced though.

Q: I would like to contribute an article for the magazine, should I write one about anonymous purchases?

A: We receive similar emails every day. You should write about whatever interests you. We can't say whether an article you write will meet the requirements for publication but we are always eager to see what you create. Don't ask, just go for it.

Q: How can we get notified of new magazine issues?

A: Per our privacy policy, we collect no details of listeners or readers. We have no newsletter or notification list. However, you can use the RSS feed available on the "Download" page within any RSS reader to be notified of each new podcast and magazine release.

Q: If I am using a VPN service, can the site I'm visiting still see my computer's MAC address? If yes, is there anything I can do on my GNU/Linux computer to shield my MAC address information?

A: No. Websites cannot see your MAC address through a traditional browser, with or without a VPN. You would need to install some specific software and grant the permission, which is still a stretch for the average user. Websites do see the IP address of your internet connection, which is where a VPN is essential. Other devices on your local network can see your MAC address. If you are staying on your trusted home network, this is probably not an issue. If you rely on public Wi-Fi networks, there could be some concern. If you leave your Wi-Fi enabled while you move around, this could track you. There are many apps which will modify your MAC address. We prefer to simply stay away from public networks when possible.

Q: I want to submit something but I need to know the deadline. When should I have it to you?

A: Whenever it is finished. There will always be the next issue which needs content. Again, don't ask, just go for it.

Q: What are some ways for young attorneys to get more into the "privacy" side of things?

A: Estate planning. Most lawyers receive very little education about trusts and ways to remove assets from public view. A competent attorney who understands state trust law deeply should see much new business in the future. An attorney could probably specialize in the art of using trusts to eliminate public exposure, especially in a large city.

Q: How I can ensure my family/friends don't fall victims to scammers?

A: Our best advice is to train others to never answer, or return, any unsolicited call or email. Any real GOV or bank problems will be addressed via postal mail.

Q: What are the best practices to have documented end-of-life instructions via a secure USB drive or online repository, so that a) it can be easily updated and b) easily accessed by family?

A: We advise our clients to talk with their families now. Explain how you have your data/instructions set up and walk them through the ways they can access. Many of our clients issue USB drives to their family to be viewed only in the event of death. The password to access the data is kept with an attorney or other family member. Both would need to cooperate to get access to the data.

Q: What do you wear to avoid being recorded? I know there are pictures that basically stops models from seeing you as a human but it works only for certain camera angles. So let's limit this to headwear and glasses to stop Clearview from adding your face to their dataset.

A: There are plenty of gimmicks which either do not work or will not work for long. Stickers, reflective clothing, and other trends don't really do much. Your best option is sunglasses, a hat, and a huge face mask. None of those are scrutinized today. I have been guilty of wearing the same shoe in two different sizes in order to impact my gait, but privacy is my hobby.

Q: What mobile Linux phones are recommended for better privacy?

A: None of them. All of our clients who have tried Linux phones became so frustrated with the VoIP calling options, that they just used their true cellular number to make and receive calls. That completely contradicts any type of privacy or security. We prefer un-Googled ROMs over any Linux option for most users.

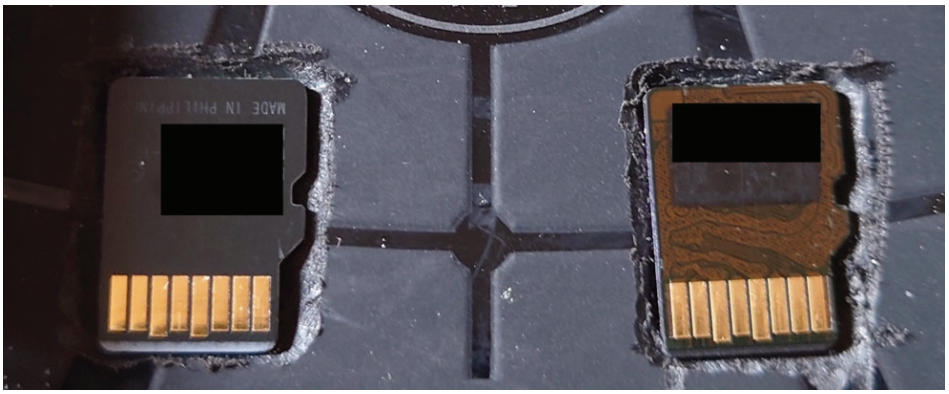
SD CARD BACKUP STORAGE

By Michael Bazzell

If you have read my books, you already know I am overly prepared for data failure. Multiple backups are a key part of my data storage policies. I have all of my documents secured within an encrypted container on my laptop for daily use. I possess a daily synchronized copy within an encrypted USB drive in the event of primary disk failure. I have a weekly backup to an external drive which is secured in a large safe in the event of theft of my laptop. I have a quarterly offline backup stored at another location in the event of disaster at my home. This should be enough, but I am paranoid about losing content. What if I have vital data created since the previous offline synchronization which is lost due to disaster? I had a need for an additional backup of my most important data which could be with me at all times.

I considered a USB drive in my vehicle, but what if it was also destroyed during a fire while away on international travel? I know that sounds ridiculous, but bad things happen. I considered a USB drive on my key ring, but those can be easily lost or damaged. I wanted a solution which would guarantee that a stable backup was always with me when I left the house, regardless of the scenario. I decided that my phone was the best option. It is always with me regardless of destination. However, I use a GrapheneOS device which does not possess a microSD card port or enough internal storage for my documents. No problem, I will make my own storage solution.

I purchased a Spigen Rugged Armor (https://amzn.to/3xP245n) protective case for my Pixel 4a. I placed four microSD cards on the interior of the case and outlined each with a pencil. I then attached a pointed grinding stone bit to my Dremel tool and began carving out my new microSD card storage slots. I can now place four 256GB microSD cards in these indentations, between the case and the phone, which provide one Terabyte of offline storage for anything I need. I never remove my phone case, so they should stay in place until I need them. Since I grinded out enough of the case, the cards lay flat and do not bulge out the back. Make sure you place them on the thickest part of the case so you do not grind through it! Below is a partial image.



This magazine serves as a compliment to the weekly podcast, which can be found at IntelTechniques.com. Below are summaries of the episodes from last month.

256-Extreme Privacy Fatigue

Announces the latest edition of Extreme Privacy and discusses ways to deal with privacy fatigue.

257-Early Warning

Discusses the risks of data sharing from Early Warning and presents a new concern about privacy-themed companies accessing your email.

258-UNREDACTED Magazine

Announces this privacy-themed magazine and presents a warning about using Telnyx.

259-Leaving Kindle

Explains how to leave Kindle's invasive e-book ecosystem with the help of large-screen Onyx BOOX readers.

SUSTAINABLE SIGNALS

By Steve Shillingford

I live in one of those "fastest growing" metros in the United States. Living in the city is a first for me; always been a suburb or rural person. I love it very much but have developed a few new skills that I didn't realize I had. They're rooted in evolution and come in handy when facing unknown people.

Every morning, usually before the sun comes up, I walk to my local gym. Somewhere between 5 am and 6 am, the crowd is sparse. Depending on the day, it's either people walking their dogs, heading to work, or if it's the weekend, leaving a bar. When I walk by these folks, I find myself auto-scanning: How are they dressed, how are they walking, headphones in or out, do we make eye contact, are they walking towards me or passed me, are they swinging a baseball bat in the air? It all happens in a second or two and I would submit it is biologically wired. We, like all animals, use the signals from other creatures to drive our "Fight, Flight, or Freeze" decisions. Whether in a city filled with strangers or the Serengeti, humans and animals access the same basic lizard brain functions to determine levels of security and safety.

Fast forward to 2022 and the Internet broke when Elon Musk acquired Twitter and said he would "fix" it by making users verify their identities. Ignore the "how" for a minute and think about what he's trying to solve. Users on Twitter and other platforms hide behind names like @Sunny @McSunnyFace or @catturd, to hide their real identities. They do it because it allows some freedom from tyranny of the majority or minority (pick your side). They do it so they can write freely about topics that may or may not be controversial. It works well and some guys did it 250 years ago very successfully. What Mr. Musk is trying to point out is the missing link in the digital world: There needs to be some consequence to one's actions online.

But wait, isn't that the problem? Anonymous people can say anything and since we live in a world where "words equal violence," we must monitor these folks. Wrong. Anonymity is critical to free expression and to the community of ideas and the public commons. To have that level of discourse, you either submit to tyranny or to freedom. Tyranny, regardless of who is in power, is no good, and in the history of the world, has never ended well. Freedom, liberty, and the "right to be let alone" is the only sustainable way to manage diversity. One has to accept that not everyone thinks like I do. Instead of stifling the debate, we need to protect it. To do that, you have to provide signals. You have to know you're having a conversation with a reasonable person and not a psycho. You have to be willing to share, hear, and exchange in a universally accepted environment. In the analog world, I buy from people and companies I trust. I accept new ideas, wisdom, and learning from sources I trust. That trust comes from the signals these people and entities send me. I assess, analyze, and act. That's my control.

Signals are very important in the world, period. In the analog world, we use signals to assess danger. We also use them to assess competence (e.g., does he speak "gooder" or "well?"). We use them to assess quality (e.g., is the office clean or dirty?). We use them to determine compatibility (e.g., long hair, short hair, fat, thin, tattoos, piercings, etc.). These signals are fungible in that they are attached to the person whether they're at work, home, out in public, or alone. Some are intentional. I walk with a hoodie and all black. Some are unintentional (or maybe not). If you know what RBF stands for, you know.

We file these signals away in the memory banks and over time, they form a reputation. "That guy is a pain" or "she's always so helpful." I have a cashier I find happy and helpful at the grocery store. I will wait in her line, even if it's longer. I have no idea what her name is. It's not about "are you human?" Rather, it's about your reputation.

In the digital world, it's different. Sure, I can get reviews on an item I want to buy. I can also get reviews on places I want to visit, have a meal, or stay for a vacation. The problem is reviews of users is very difficult, if not impossible, to assess. Sure, a blue check twitterati might indicate real humans, but what does it say about the veracity of their posts? Do they propagate BS or do they offer interesting historical facts? Provocative or thought-provoking? Do they start the tweet-storms or do they try to put them out?

Signals have been a sustainable method for assessing risk, security, safety for thousands of years, yet we have

nothing close to it for identities in the digital world. Why not? We need a way to leverage digital reputations the way we leverage analog reputations. We do not need a way to "verify" humans. Verifying a human is a coarse-grained approach and the intent is directionally correct, but it will not work. Just like the "fact-checkers" are fails, verifying a human is impossibly difficult in the digital world. Impossible, unless you demand government-issued identification. But what makes us think we can do this as private companies? It will only get hacked, tracked, and harvested just like the rest of our data.

I won't go into why privacy matters. It's obvious and historical, and anyone who argues against it is either lying or manipulating you. Follow the incentives.

Give people privacy but demand the portable digital reputations that allow us to assess signals of identities the same way we solve for this in the analog world. I don't need to know whether you're "verified." I need to assess whether you're a source I trust.

Lots of ways to solve this. I think there's a patent or two about it somewhere. The point is having a consequence for an action. The reason the online world, including places like Twitter, are cesspools for a-holes is because users can hide behind a powerful combination of anonymity and consequence-less action. In the analog world, I can criticize my government all I want. I can even send my Senator long manifestos about his terrible voting record. But have you tried to send your representative an email without including your name, address and phone number? If you have, you know it's largely impossible at the Federal level. And if you do, you know your "manifesto" turns into a politely-worded "I strongly disagree" so as to avoid 29 armed agents showing up at your door at 4 am. Just saying.

The important point here is not that every human needs to be verified. In fact, it's quite the opposite. What we love about Michael Bazzell's podcasts and this online magazine is his devotion to helping us protect our identities…regardless of how many we choose to have. But, having multiple identities, like I have multiple personas, shouldn't prevent me from posting or reacting. Even if that comment is not mainstream. There should just be a consequence. Are you a jerk? Downvote, one star, something. Great idea? Upvote, five stars!

Just like there's a consequence for yelling at the guy on your grass, cutting off the stranger on the freeway, or offering your seatmate your almonds, there should be a consequence for actions in the digital world.

PRIVATE USA PASSPORT RENEWAL

By Up

This guide is intended to serve as an outline for submitting the most 'private' version of a United States Passport Renewal application possible. There needs to be a clear understanding this is a Government document, so we are NOT using FALSE information. Just safer information that is accurate. I recently renewed my United States Passport. I did not have a passport card, just the book. I wanted the card for use in place of my State issued Driver's License when being asked to show ID. To obtain the card, you must renew your valid US Passport Book. If you don't have a US Passport, you will need to apply for one. I wanted to use information that would not harm me should it become public. I am not attempting to 'hide' from the Government. I believe I shouldn't be forced to reveal information that, conceivably, could be used to harm me. The Application can be found at https://eforms.state.gov/Forms/ds82.pdf.

I reviewed the renewal application for quite some time trying to figure out which boxes to fill out, which to leave blank and what information I wanted to populate in each box without lying. The following is the most minimalistic approach for my circumstances while providing accurate information. Note that the first four pages are not required.

Box 6: Create a single use email address. They will associate this email with YOU and should there be an issue they can email you. You can also receive application status updates by providing an email address, but I never did.
Box 7: (Leave Empty) - I did not provide a phone number.
Box 8: (Fill) & Box 18 (Leave Empty) - I used a PMB address. They ask for an address but specifically state later on Box 18 "Do not list a PO Box". A PMB is not a PO Box.
Box 15: I recommend leaving something generic in this box that is applicable to your line of work such as Consultant, Admin, Medical, etc. When you pass through customs they will often times ask "What is your occupation?" as a form of validation. Best to give them a simple answer in my view.

Visit https://travel.state.gov/content/travel/en/passports/how-apply/photos.html and review all requirements for a passport photo. If you have the equipment to do this yourself, you should. I elected to use a 3rd party to take and print my photograph. Many places that offer typical 1hr photo services also offer Passport photo services. Once the picture is taken they will remove an SD card from the camera and insert it into a computer for editing images. The software used has the ability to detect images which will better meet the requirements. You might be asked for your name and phone number, but simply refuse.

There are 3 processing options to choose when applying for renewal, with the following current expected delivery:

Routine: 8 to 11 weeks
Expedited: 5 to 7 weeks
Expedited Agency: 3 days with international travel booked

Once you determine your fee, you will either need to pay by check or money order. I recommend to pay by money order. While in a location far from home I picked up a money order for the exact amount owed paid for in cash. There was no need to show ID to make the purchase. You will need to list the following on the Money Order:

Payable to "U.S. DEPARTMENT OF STATE"
Print FULL NAME
Print DOB

You will need to mail the application with photo attached, payment, and most recently issued Passport and/or card inside an envelope to the correct address for the level of service you require. Refer to PG 1/4 on form DS-82 for your address based on the level of service you require. I elected to use USPS for this. I visited a location far from home, listed my PMB as return address, and paid cash for my package to be sent priority mail. This provided me with a tracking number I could use to ensure my documents were delivered. I made payment for 'Expedited' processing and '1-2 Day Delivery'. Your results may vary. Here were mine:

Day 0: Mailed Documents USPS Priority 2 Day
Day 2: Documents Delivered to Destination
Day 7: Application Portal Listed as "In Process"
Day 18: Application Portal Listed as "Approved"
Day 23: Passport Book Received at PMB
Day 25: Passport Card Received at PMB
Day 35: Supporting Documents Received at PMB

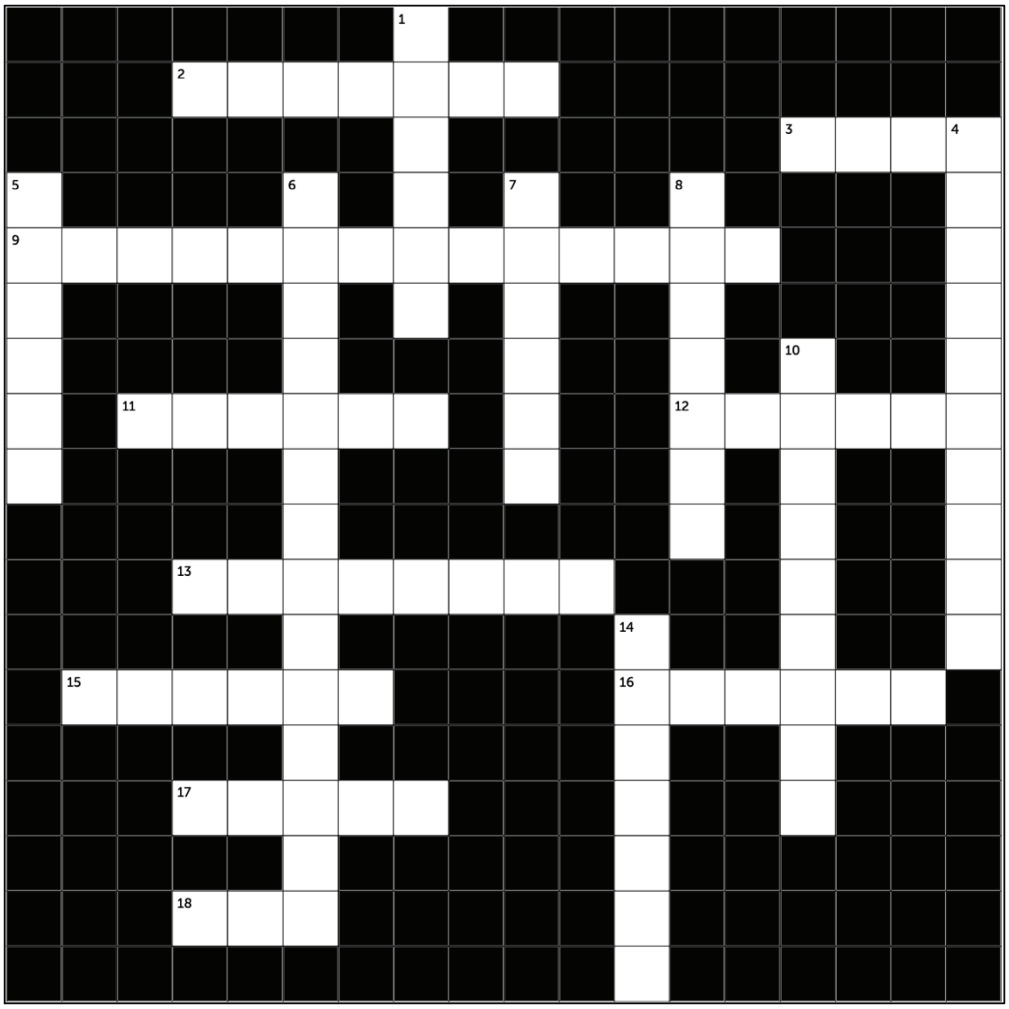
Editor's Note: *The big lesson here is to always use minimal contact details which you allow to be publicly visible if/when this data is shared, and remember what you provided when questioned so that everything matches up.*

ADVERTISEMENT

There is no ad here (yet). While we find our footing, consider sponsoring this publication with a full-page, half-page, or quarter-page ad promoting your product or service. Contact us at https://UNREDACTEDmagazine.com to see how we can help your business grow while supporting this free resource. If you are reading this, just think of the other eyes waiting for something to appear here.

PRIVACY-THEMED CROSSWORD

By Anonymous



Across

2 Popular Virtual Currency
3 Plant Your _____
9 Sole _____ (Self-Employed)
11 Popular Linux Version
12 Credit _____
13 Blocks Outgoing Connections
15 Secure Messenger App
16 Apple Tracking Device
17 Open Source Intelligence Acronym
18 Masks IP Address

Down

1 Current Edition of Extreme Privacy
4 Google-Free Android ROM
5 Remove Data From Company
6 Intentionally Wrong Details
7 Android Debug ____ (ADB)
8 Browser Alternative to Chrome
10 Sending of Usage Data to Service
14 Bag to Block Signals

Editor's Note: *We are always looking for privacy-themed puzzles including crossword, word find, and anything else you might create. Send us your best submission.*

FINAL THOUGHTS

By Michael Bazzell

Well, how did we do? I suspect some readers are answering with "You should have discussed ____." or "Why don't you write about ___?", which is where you come in. Let us know how we can improve by sending your own submissions for publication. This issue was only 30-ish pages, but I hope to double the content soon.

I sincerely thank everyone who contributed to this inaugural issue. From announcement to publication was only two weeks due to my competent and talented staff, and the contributors who sent content. My goal is to present another issue in June, but only you can make that happen. I look forward to seeing what you come up with next.

~MB

CROSSWORD ANSWERS

Across

2 BITCOIN
3 FLAG
9 PROPRIETORSHIP
11 UBUNTU
12 FREEZE
13 FIREWALL
15 SIGNAL
16 AIRTAG
17 OSINT
18 VPN

Down

1 FOURTH
4 GRAPHENEOS
5 OPTOUT
6 DISINFORMATION
7 BRIDGE
8 FIREFOX
10 TELEMETRY
14 FARADAY