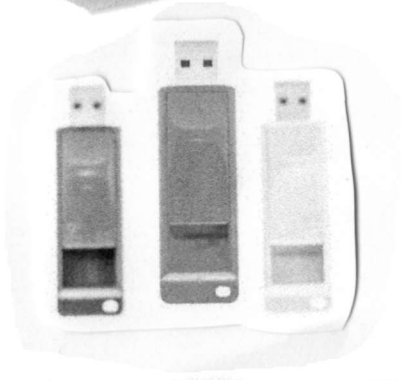
Sneakernet!



This was zine created by Adam McFillin for *Circuitous City* as part of Outer Space's *Into the Ether* series. Visit circuitous.city for more information.

WHAT IS A SNEAKERNET?

A sneakernet is a network created by transferring data physically instead of over a computer network. Sneakernets can be as formally or informally organised as you like, and can make use of any kind of storage device.

The most literal example of a sneakernet would be in the form of a human being carrying a disk, travelling on foot—hence the ‘sneaker’ part. I doubt your choice of shoe really matters, other than the fact that sneakernet sounds like Ethernet, which probably sealed the deal on bringing the name into popular usage.

Sneakernets are almost the opposite of the internet in that, on the internet, every device needs to communicate via the same set of protocols, and those protocols are used to route your messages from source to destination via the most efficient (efficient for who though? More on that later) path.

On a sneakernet though, you can make your own rules. You can encode your information into whatever digital or analog format you like; hard disk, paper, cassette tape, USB key, CD, whatever. You can then transfer your data however you like; on foot, on a bike, cross-country skiing, in a taxi, in a bottle set adrift on the ocean!

The extra added bonus to sneakernets is that if you carry enough information with you—say a few terabytes on a portable hard disk—there’s a chance that you can get the data to your destination quicker than sending it over the internet! More on this later in the zine, too.

WHY SNEAKERNETS? WHY OFFLINE NETWORKS?

There are probably as many reasons why someone might choose to transfer their data offline as there are ways to create a sneakernet, but some of the popular ones are:

- **Convenience**: Sometimes it's just easier or quicker to hand the information to someone in another part of your house, building or city—especially if you don't have a home network, or one or both of you don't have especially fast, reliable, or affordable access to the internet.
- **Speed**: This could potentially be considered part of convenience, but I'm not sure loading hard drives on/off shipping containers or sending out pigeons is really **that** convenient.
    - Sneakernets are often used for huge-volume data transfer. We're talking moving huge databases or even whole data centres at once here. Radio telescopes like the Hubble apparently create huge amounts of data, too, and moving that data physically is simply the quickest way of getting it from point A to point B. Amazon even has a branded service for this – AWS Snowball.
    - In the 2000s, a few experiments were performed (assumedly by people less than thrilled with the speed of the home ADSL internet connection) racing a messenger pigeon carrying a USB stick or SD card against an ADSL connection transferring the same data. In each case the pigeon won easily.
    - Even early internet pioneers were well aware of the potential "bandwidth of a station wagon full of tapes hurtling down the highway". This quote has been attributed to many early internetworkers, including Andrew S Tanenbaum, whose 1981 textbook asks students to calculate the data transfer rate of a St Bernard carrying floppy disks.

- **Privacy or secrecy**: In 2020, everything you do on the internet is likely under surveillance in some way or another. In Australia, there are federal laws (search: Australia data retention) that require all Internet Service Providers to collect information about where their customers go online. This is in addition to Edward Snowden's 2012 revelations that not only is Australia part of the Five Eyes coalition—a group of countries that share digital surveillance information between each other—but that online communications between US citizens and foreigners is captured and available to NSA analysts without a warrant.

  Our American neighbours are doubly lucky in that their ISPs are also allowed also sell their customers' web browsing data and history without their consent.

  And needless to say, if you're sending information using social media platforms from anywhere in the world, that's being used to sell ads, too.

  So if you're not into your data being at risk of surveillance or interception, taking it directly to someone you trust in person might be the most effective solution.

FAMOUS SNEAKERNETS AND OFFLINE NETWORKERS

- **El Paquete Semanal** (translation: "The weekly package") is a 2 TB hard drive of the latest, movies, TV shows, music and more, compiled and distributed by a huge human network throughout Cuba. You can even just BYO USB stick to your local *paquetero*, who will allow you to select parts of the package that appeal to your tastes or suit your budget. Each new *paquete* reaches 90% of the Cuban population within 48 hours of it hitting the streets, making it far more effective than the expensive, slow, and heavily censored internet access available to most Cubans.

- **Edward Snowden** smuggled surveillance secrets out of the NSA on a USB drive.

- **Chelsea Manning** snuck secret Iraq and Afghanistan war logs out on rewritable CDs labelled 'Lady Gaga' and later copied those files on to her camera's SD memory card to transport them into the US.

- Regular ol' **Mail** is also pretty effective! Of course, any kind of communication – printed media, spoken word, etc. - has a human network element, and while this zine only talks about digital data in the form of computer files, you could easily extend the concept back to the history of messengers, Australian indigenous songlines, printing, shipping and trade, and more.

DEAD DROPS

If you want to add a dash of intrigue or secrecy to your sneakernet, consider an anonymous transfer via dead drop.

Dead drops have their background in espionage, where agents leave objects in a secret agreed-upon location to be picked up. This is opposed to a live drop, where two people just hand each other the object in person. Doing a dead drop helps preserve agents' identity and lessens the risk of the handoff being seen by onlookers, adding some security to the transaction. However, it also introduces the risk that the object may be found or interfered with by a member of the public. Dead drops are also sometimes used by reporters and their sources.

These days, USB dead drops—USB keys wedged into places like holes in walls, bricks or trees—are popular with geocachers, who make a hobby out of hiding and finding objects in locations that are challenging to access, or identified by co-ordinates that need to be deciphered like a puzzle. Pirate Boxes—small WiFi routers that allow for anonymous file sharing—are also a popular way of providing a dead drop-like experience. Check deaddrops.com to see if there are any active dead drops in your area.

WHY NOT?

When making a choice about how to send data, we are often trading one set of problems for another, and the decision to transfer files offline is no different. Some of the common problems with transferring data offline are:

- Storage media gets lost or dropped.
- Storage media gets damaged and its contents are corrupted.
- Storage media gets passed on to someone you didn't intend it to.
    - Once you hand it on to someone, it's out of your control. What if you need a middle-person to get things from A to B? How do you know you trust them?
- Storage media gets infected with a virus.
- Interpersonal conflict! You have a fight with the person you relied on to send or receive data with.
- Miscommunication – you fail to meet up at the right time/place.
- The person you gave the data to was not trustworthy.
- The person you received the data from was not trustworthy and/or put a virus or malware on the storage media.
- The other people in your network have different ideas about how the network should run, how important the information is, and how the information should be used.

BIG DEAL. WHAT'S SO AMAZING ABOUT GIVING SOMEONE A BUNCH OF FILES?

*(AKA MY ANNOYING NEIGHBOUR IS ALWAYS TRYING TO GIVE ME 2 *TERROR*BYTES OF HIGH-DEF LIVE RECORDINGS OF JAM BANDS AND I'M REALLY NOT INTO IT)*

Here are some reasons:

- Forms of communication that subvert governmental surveillance are important! If not for you, then for those who need it to maintain their safety, privacy, or just for the hell of defending the principle that our communications shouldn't be spied on at all times, or sold for someone else's profit.

  It's a bummer that it's come to this, but your well-meaningly enthusiastic but annoying neighbour is now basically a subversive radical hacker and it's worth considering whether you should take a leaf out of their book if you ever have Top Secret Business to attend to, or just want to make your own personal demonstration of defiance.

- The internet is designed for efficiency; that is, getting your message from point A to point B in the fastest possible time. Why? Because it makes service and content providers the most money.

  Providing you, the demanding consumer with reliable, low latency, high bandwidth data transfer works entirely in their interest and helps keep you glued to the screen thanks to flawlessly streaming movies or the instant gratification of real-time likes and comments on your latest post. They don't care whether your data crosses national boundaries that cause it to be snooped on, they don't care if it travels through (potentially supporting the economies of) countries that violate human rights (but if they did, sorry Australia, no internet for you), they don't care that the company that owns those huge long undersea cables may actively support sexism in their workplace or profit from the unlawful detention of asylum seekers.

What I'm getting at is that sneakernets (and by extension, other non-internet networks) give us the opportunity to (to use the techbro-iest of terms) 'optimise for' something other than the conventional, economically-defined notion of performance.

You can 'optimise' your sneakernet for whatever values are important to you. You might want to share information with groups of people who you know support indigenous or refugee rights, you might be interested in meeting people in your local neighbourhood, or fellow fans of your favourite soccer team. A local sneakernet could help you do that! Perhaps you want to share secret information—like evidence of your shady landlord, or your grandma's recipes—only with those you trust. Handing a password-protected USB key around a group of friends can allow you to do that, too.

Maybe doing a sneakernet drop-off is a good excuse for you to go on a nice walk or bike ride to a friend's place? Optimise your network for thoughtfulness by including a couple of songs that reminded you of them, or an article, or essay or poem you wanted to share. Maybe have that friend add some more songs and pass it on to another friend? None of this needs to be formal and there don't need to be any rules. Maybe you just feel like doing something different?