

# Perils of the cashless society

Invited Lecture

ESTA Conference, October 24 - 26th 2021, Sevilla, Spain

**Domagoj Sajter**

Full Professor at Faculty of Economics in Osijek, Croatia

Chair of the Department of Finance and Accounting

e-mail: [sajter@efos.hr](mailto:sajter@efos.hr), mobile: +385 91 2244 102;

web: <http://www.efos.unios.hr/sajter>

## Keywords

cashless society, privacy, democracy, anonymity, freedom

## JEL Codes

E42, E44, E59, G21, G28, O33

## 1. Introduction

In the context of covid-19 pandemic it was expected and understandable that, after the initial shock of lockdowns and standstill of the world economy, many players – both large global corporations and small local entrepreneurs – were looking for new ways to make use of the extraordinary circumstances to their benefit. Entrepreneurs are agile; they quickly find ways to swim in the new waves of the change/pandemic<sup>1</sup>. Among them are financial institutions, who, without credible previous research, quickly began to push for the rejection of cash as a supposed carrier of coronavirus.

Even without and long before covid-19, statistics clearly showed the long-term trend of diminishing influence of cash in the economic system. Approximately 300 ATMs were being shut down in Britain monthly, leaving consumers without access to cash, according to a [report](#)<sup>2</sup> from a Consumers' Association. About 8% of ATMs were being closed every year in [Australia](#)<sup>3</sup>. In 2017 more than 1150 ATMs

---

<sup>1</sup> In doing so, many conspiracy fans make the logical mistake of “*post hoc, ergo propter hoc*” by reasoning: if these entrepreneurs profit in a pandemic, it must be that they deliberately created it.

<sup>2</sup> <https://www.telegraph.co.uk/money/consumer-affairs/three-hundred-cash-machines-disappearing-month-leaving-villages/>

<sup>3</sup> <https://www.news.com.au/finance/money/costs/definitely-here-to-stay-most-people-still-withdraw-cash-from-an-atm-at-least-once-a-month/news-story/caf9739caccceade6655adbeacec34b1>

were permanently closed in [Spain](#)<sup>4</sup>, where all of the largest banks cut access to cash. These kinds of numbers can be observed almost everywhere.

Nevertheless, there is a larger context of scrapping physical money; one that includes global technological and financial giants, as well as large commercial and central banks, and their vested interests. They have a lot to gain from citizens abandoning cash and switching to payment instruments and systems which they control, and from whom fees and data can be collected. Furthermore, vast amounts of the ultimate resource of the postmodern era - data - can be extracted and resold. Cash represents direct interchange, power in the hand of the holder and autonomy of participants, while cashless transactions can only arise if prerequisites are taken into consideration (power supply, internet connection, hardware and software, etc.), and only with intermediaries, their fees and data harvesting.

Regrettably, the discussion regarding cash is far from balanced; there are many strong and vocal [opponents](#)<sup>5</sup> to cash, but very few voices that speak on behalf of it. It is argued here that cash is an essential instrument for establishing a genuinely free and democratic civilisation. Materially, cash is the most powerful invention (or tool) homo sapiens has ever made; nothing comes close to it.

This lecture is a part of a continuous effort (Sajter, 2014a, 2014b, 2021) to keep cash as a legitimate and precious instrument of a free society with empowered citizens. After this introduction, through a mosaic of cases we will delve into current state of new technologies that strip citizens of their privacy. Next, we will also discuss “positive” aspects of the disruption and look behind the forefront of the arguments. A sum-up of the threats of the cashless society follows, together with the conclusions.

## **2. Changing landscape: sleepwalking into cashless society?**

The world has always been a changing place, but there are many signs which indicate that the pace of change has significantly sped up and is beyond the comprehension of a common cash user.

According to some sources, Apple plans to install software on its newest phones to detect child abuse images. On the face of it this move seems non-controversial and praiseworthy. However, it raised alarm among security researchers who warn that this could open the backdoor to surveilling millions of people's personal devices; [experts](#)<sup>6</sup> claim that if recalibrated, the system could be

---

<sup>4</sup> <https://www.economista.es/empresas-finanzas/noticias/9328737/08/18/Los-bancos-eliminam-de-1000-cajeros-automaticos-en-solo-un-ano.html>

<sup>5</sup> e.g. <https://time.com/4918626/money-germs-microbes-dirty/>

<sup>6</sup> <https://www.ft.com/content/14440f81-d405-452f-97e2-a81458f5411f>

adapted to detect anything, e.g. anti-government signs at protests; whatever imagination can come up with.

In [Australia](#)<sup>7</sup>, until recently one of the freest countries in the world, government introduced the obligation to install a specific smartphone application, in addition to the imposed lockdown. Citizens who travelled within the country must be quarantined and are forced to install this app that combines facial recognition and location via satellites. The agency sends them a message; after that, a person has fifteen minutes to make a selfie in the location where he should be. If he fails, the police is sent. Also, the [military](#)<sup>8</sup> is sent as it patrols between the states. It doesn't surprise that Australian institutions are determined to eliminate cash from the economy, and are enacting Orwellian [laws](#)<sup>9</sup> that allow unprecedented monitoring of citizens.

Facebook's business model is essentially harvesting user data and selling it to customers who get precisely dissected target audience. In a similar fashion, [Google](#)<sup>10</sup> tracks its users' payment history; in addition to the search history it scans all the contents of the e-mail inbox (Gmail) and payments through its platform (Google Pay). What is there to be gained? Every click counts, and every click, along with every payment with a card - be it "classic plastic", or through NFC technology in mobile phones or smart watches (contactless) - creates a mark in the big data. These are massive data sets used primarily by large corporations to detect trends and patterns in consumer behaviour. Big data is a treasure cove, and going over it is literally dubbed mining (as in mining for precious metals) because it can struck gold: detailed consumer profiles. Two people *googling* for exactly the same keywords will not get the same results; this is because they are tailored to the user's profile. In this way, users are kept in somewhat of a "golden cage"; they think they are free to choose, but in fact they choose between what technological giants have pre-selected for them. This is hardly freedom – it seems more like a manipulation.

To illustrate previous statements, news was collected from well-known and widely used internet outlets regarding issues of consumer privacy. In a brief time-period (from the beginning of November 2018 to end of January 2019) there were many accounts of malfeasances with user data (Table 1.). This calls for a wider introspection:

*“The recent increase in reported incidents of surveillance and security breaches compromising users' privacy call into question the current model, in which third-parties collect and control massive amounts of personal data.”* (Zyskind et al., 2015, p. 180)

---

<sup>7</sup> <https://www.theatlantic.com/ideas/archive/2021/09/pandemic-australia-still-liberal-democracy/619940/>

<sup>8</sup> <https://unherd.com/2021/09/whats-the-point-of-australia/>

<sup>9</sup> <https://digitalrightswatch.org.au/2021/09/02/australias-new-mass-surveillance-mandate/>

<sup>10</sup> <https://www.fastcompany.com/90349518/google-keeps-an-eye-on-what-you-buy-and-its-not-alone>

*Table 1. Examples of malfeasances with user data*

Publisher of the news*	Shortened link to the news	"Perpetrator/-s"	Exploit
Washington Journal of Law, Tech and Arts	<a href="https://tinyurl.com/yxqjmul">tinyurl.com/yxqjmul</a>	Amazon	Consumer generated mass surveillance
Business Insider	<a href="https://tinyurl.com/y3be8jk6">tinyurl.com/y3be8jk6</a>	Amazon	Spying/tracking users
Financial Times	<a href="https://tinyurl.com/y2yzzh2n">tinyurl.com/y2yzzh2n</a>	At least 34 apps (games, etc.)	Selling user data to Facebook
New York Times	<a href="https://tinyurl.com/y7lry8rw">tinyurl.com/y7lry8rw</a>	At least 75 companies	Spying/tracking users
Techcrunch	<a href="https://tinyurl.com/y9h3ky78">tinyurl.com/y9h3ky78</a>	Facebook	Spying/tracking users
35th Chaos Communication Congress	<a href="https://tinyurl.com/y3ja6w83">tinyurl.com/y3ja6w83</a>	Facebook	Tracking and selling user data even if user doesn't have FB account or app
Ars Technica	<a href="https://tinyurl.com/y3yby6ya">tinyurl.com/y3yby6ya</a>	Facebook	"Knowingly violated" privacy laws
The Verge	<a href="https://tinyurl.com/yckq85tt">tinyurl.com/yckq85tt</a>	Facebook	Spying/tracking users
Wired	<a href="https://tinyurl.com/y7o9muqb">tinyurl.com/y7o9muqb</a>	Facebook, Instagram, WhatsApp, Messenger	Sharing user data
Business Insider	<a href="https://tinyurl.com/y7e9gbcn">tinyurl.com/y7e9gbcn</a>	Google	Creating "bubbles" by filtering search results
Deutsche Welle	<a href="https://tinyurl.com/yyazasz">tinyurl.com/yyazasz</a>	Google	Privacy breach
Techcrunch	<a href="https://tinyurl.com/yaopxlop">tinyurl.com/yaopxlop</a>	Google	Spying/tracking users
Medium	<a href="https://tinyurl.com/ydfmnbpe">tinyurl.com/ydfmnbpe</a>	Google	Spying/tracking users
Medium	<a href="https://tinyurl.com/yjwzjh7">tinyurl.com/yjwzjh7</a>	Google	Spying/tracking users
The Intercept	<a href="https://tinyurl.com/yagqxlh7">tinyurl.com/yagqxlh7</a>	Google	Spying/tracking users
Business Insider	<a href="https://tinyurl.com/y3jb37ac">tinyurl.com/y3jb37ac</a>	Google	Secretly putting microphones in devices
Search Engine Journal	<a href="https://tinyurl.com/y4uayhns">tinyurl.com/y4uayhns</a>	Google, Facebook, Twitter	Disrespecting the "Do Not Track" setting on web browsers
Bruce Schneier	<a href="https://tinyurl.com/y8yy9eh9">tinyurl.com/y8yy9eh9</a>	Government/-s	Placing surveillance cameras in streetlights
Wired	<a href="https://tinyurl.com/y7r24mel">tinyurl.com/y7r24mel</a>	Governments	Spying/tracking citizens
Fair	<a href="https://tinyurl.com/yg47urs">tinyurl.com/yg47urs</a>	Governments	Potential misuse of face recognition
Motherboard	<a href="https://tinyurl.com/ya25y9wx">tinyurl.com/ya25y9wx</a>	Hundreds of free apps	Tracking and selling user data
Boing Boing	<a href="https://tinyurl.com/yadvbxv">tinyurl.com/yadvbxv</a>	Lifx	Passwords saved insecurely (in a lightbulb)
Bloomberg	<a href="https://tinyurl.com/y9jzrjmf">tinyurl.com/y9jzrjmf</a>	Private DNA testing company	Leaking DNA data to FBI
Business Insider	<a href="https://tinyurl.com/ybjldmrg">tinyurl.com/ybjldmrg</a>	Smart TVs	Tracking and selling user data
Bleeping Computer	<a href="https://tinyurl.com/y49o9jr5">tinyurl.com/y49o9jr5</a>	Thousands of apps	Violating policies
Techcrunch	<a href="https://tinyurl.com/y49o9jr5">tinyurl.com/y49o9jr5</a>	Unknown	24 million financial and banking documents published online

*\*News published during the three month period from the beginning of November 2018 to end of January 2019*

Source: (Sajter, 2019)

The chaotic global pandemic has exacerbated and intensified previous trends. In this context, pressed to renounce certain liberties in exchange for a

hunch of security, the economic entities seem to be sleepwalking into cashless society.

### 3. “Positive” aspects of cashless society

Eradication of cash would certainly bring some benefits to the society, but at what costs? The arguments for the suppression of physical money are always the same; they include some form of cash denigration coupled with carefully framed “positive” aspects.

First and foremost, abolition of cash is marketed as a fight against underground economy; against illegal trading of weapons and drugs, trafficking, money laundering, tax evasion, and other black market activities. It is argued that terrorists could be restrained if identity of the transaction parties can be revealed. With cash out of the window anonymity and privacy of the market participants would be lost, which would lead to more effective law enforcement. Certainly, no one reasonable could be against these endeavours?

However, the largest volume of the money laundering and tax evasion is performed by large banks<sup>11</sup> and multinational corporations<sup>12</sup>, not by citizens. They are in a position to (successfully) lobby<sup>13</sup> for the legislation which permits them to evade tax<sup>14</sup>. The sheer existence of offshore havens exhibits triumph of tax evaders and money launderers. On the other hand, terrorism is mostly financed by certain sovereign countries<sup>15</sup> and intelligence agencies: top-down, not bottom-up. There has always been a trade-off between freedom and safety, and elimination of cash is a follow-up to the manufactured perception of inflated insecurity.

Secondly, holding any amount cash is ridiculed as irrational because cash is prone to stealing. It is said that when there is no cash there is no object of theft, which should lessen the level of criminal activity.

Nevertheless, criminals can steal credit cards and intercept online payments as well as they can steal a purse. With the extinction of cash, offenders are merely migrating from the tangible world into virtual sphere. It should be noted here that providing security in cash management is relatively simple and inexpensive in comparison to providing security in a digital economy; cash transactions do not require constant power supply and internet connection, 24/7 customer service, continuous updating of protection systems against all new kinds of malware and

---

<sup>11</sup> <https://www.icij.org/investigations/fincen-files/global-banks-defy-u-s-crackdowns-by-serving-oligarchs-criminals-and-terrorists/>

<sup>12</sup> <https://blogs.lse.ac.uk/businessreview/2020/09/29/how-multinationals-circumvent-anti-tax-avoidance-regulations/>

<sup>13</sup> <https://www.nytimes.com/2021/09/19/business/accounting-firms-tax-loopholes-government.html>

<sup>14</sup> Lobbying by tech giants increased by 510% between 2014 and 2019. (Source: EU MP, <https://twitter.com/AlexandraGeese/status/1217506731070296064>).

<sup>15</sup> <https://www.politico.com/f/?id=00000154-cefd-d467-ab5f-eeff521b0001>

viruses, alternate servers on backup locations, sophisticated surveillance and monitoring, etc.

Thirdly, in the context of security, it is often brought up that paper and metal money carry bacteria and viruses<sup>16</sup>, recently the novel coronavirus as well. Fear mongering of “dirty cash” in the times of covid-19 certainly pushed further towards cashless society; after the pandemic started in some retail chains in Croatia shoppers are constantly called over speakers not to pay with cash. Mastercard argued that “*using cash is extremely risky*” (position paper from 15th April 2020) and urged to switch to contactless payments.

At the same it is overlooked that cash is permanently immune to all known and yet to be imagined *digital* viruses, spyware, worms, trojans, and other malware. Germs can be easily washed away with soap, but risk management in the age of super-computers and optical fibers is far more complex and costly.

As for the coronavirus, the Bank of England commissioned a [research](#)<sup>17</sup> to understand how the virus behaves on banknotes. In this study a high dose of the virus was applied to a banknote to allow for a controlled understanding of how the virus declines with time on surfaces. This was probably a worst-case scenario, representative of someone coughing or sneezing directly onto a banknote. The results are consistent with other early studies, where a rapid decline was observed over a number of hours, and suggest that the risk of transmission via banknotes is low. Additionally, a research done for the ECB “*shows that the SARS-CoV-2 virus is only transferred from cash to the human finger in very low quantities. The levels are below what would be needed to be infectious, making the risk of transfer very low*”, and it concludes that “*the risk of transmission via banknotes and coins is very low, and that cash is safe to use*” (Tamele et al., 2021).

Paradoxically, many of the activists which are opponents of vaccination and lockdowns stand ready to protest for what they perceive as human rights and basic freedoms, while disregarding the obvious battle for the ultimate and the most powerful resource: money.

#### 4. Perils: key takeaways

Financial eco-system is undergoing an unprecedented experiment: implementation of negative interest rates. They are a perversion *sui generis* of financial technocrats and create twisted incentives: increasing risky investments and indebtedness, while simultaneously demolishing savings and pension systems. Physical currency could be the last barrier to overarching financialization of society, as cash holds the brakes of slipping further down the slope of negative

---

<sup>16</sup> “Cash is filthy.” (Wolman, 2013, p. 34)

<sup>17</sup> <https://www.bankofengland.co.uk/quarterly-bulletin/2020/2020-q4/cash-in-the-time-of-covid>



rates. Without it there would be no limit and no possibility of a run on deposits which hold bank management accountable, attentive and vigilant.

Apart from physical currency being a backstop to endless financial engineering, cash payments cannot easily be traced; they leave no trails. Opponents of cash therefore argue that illegal activities, tax evasion, operations of diverse criminal groups and terrorists and other black market actions could be eliminated by moving to fully monitored payment system. Behind it there seems to be a mindset that every individual is a latent criminal or terrorist, worthy of continuous, omnipresent surveillance. Implicitly, everyone is assumed to be on the verge of a felony, it's just the matter of time when it will be recorded<sup>18</sup>. The pursuit of anonymity is regarded not as a natural longing for privacy and for basic human respect, but as an intention to “hide something”. Some argue that if one isn't doing anything wrong one has nothing to hide, but that is just an oversimplification of the innate conflict between the concepts of control and liberty.

There is an increased yearning for transparency and individual power in today's ever more interconnected, but at the same time alienated world, where only a handful of US companies govern and control almost entire global digital domain. Why are anonymity and privacy such important assets in the digital world we now inhabit? Cash is a tool for empowering civil liberties; it supports pluralism of thoughts in society as many people rely on it when they contribute to unpopular or sometimes controversial projects, activities, NGOs, etc. Fundamental liberties, such as freedom of speech, are at stake. Identity exposure reduces funding for unusual, difficult and contrary ideas, persons and organizations. This already manifested in December 2010 with the obstruction of funding of Wikileaks by major financial players such as VISA, MasterCard, PayPal, Bank of America and Western Union. The result is a weaker form of democracy in which many voices cannot be heard and lobbied for. When the channels of mainstream democracy are obstructed, a natural reaction is a push towards extremism, which we can now observe in the USA and elsewhere.

Tracing payments creates what we call “big data” – voluminous records of transactions. Big data benefits large multinational corporations, which use artificial intelligence (AI) to model products and services fitted to consumers' habits. The AI models are trained on the historical datasets which are used to detect patterns of past behavior, but this also creates a systemic discrimination against former self. Because future cannot be observed, historical data is used within models to predict it. Piercing this bubble seems impossible since nothing can really be deleted from the internet once it is published online, and digital giants create an eternal copy of all of our historical records. “[Metaverse](#)”<sup>19</sup> is one vision of the future; it is a virtual environment where most of our dealings will

---

<sup>18</sup> There is an estimate that a common person in the USA unknowingly commits three felonies a day, on average (Silverglate, 2009).

<sup>19</sup> <https://www.newyorker.com/culture/infinite-scroll/facebook-wants-us-to-live-in-the-metaverse>

take place, “an embodied Internet”. In the cyberspace (or “digital space”) cash is regarded as a remnant of the past, almost as a barbaric relic.

The fight for cash is therefore more than it seems. It is a campaign for physical over virtual, for tangible over digital, for real over abstract, for human contact over cybernetic simulation. It is not a Luddite combat against progress, but a struggle to sustain and preserve an important component of natural human relations. Fundamentally, it is a commitment to uphold individual power and liberty.

## Bibliography

- Sajter, D. (2014a). *Petition for a free choice of the payment instrument type*. Change.Org. <https://www.change.org/p/hrvatska-udruga-banaka-zaslobodan-izbor-vrste-kartice-pla%C4%87anja>
- Sajter, D. (2014b). Privacy, Identity, and the Perils of the Cashless Society. In *Kultura, identitet, društvo—Europski realiteti* (pp. 160–170). <https://www.bib.irb.hr/634414>
- Sajter, D. (2019). Unblocking Blockchain Potentials. *Book of Proceedings from the 2nd International Scientific Conference on Digital Economy - DIEC 2019*, 13–20.
- Sajter, D. (2021). Sleepwalking into cashless economy. *Prilika, mjesečni prilog Glasa Koncila, 9 / 2021*. <https://www.bib.irb.hr/1147182>
- Silverglate, H. A. (2009). *Three felonies a day: How the feds target the innocent* (1st American ed). Encounter Books.
- Tamele, B., Zamora-Pérez, A., Litardi, C., Howes, J., Steinmann, E., & Todt, D. (2021). Catch me (if you can): Assessing the risk of SARS-CoV-2 transmission via euro cash. In *Occasional Paper Series* (No. 259; Occasional Paper Series). European Central Bank. <https://ideas.repec.org/p/ecb/ecbops/2021259.html>
- Wolman, D. (2013). *The End of Money: Counterfeiters, Preachers, Techies, Dreamers--and the Coming Cashless Society*. Da Capo Press.
- Zyskind, G., Nathan, O., & Pentland, A. ‘Sandy’. (2015). *Decentralizing Privacy: Using Blockchain to Protect Personal Data*. Ieee.



# Perils of the cashless society

prof. Domagoj Sajter

Faculty of Economics in Osijek, Croatia

sajter@efos.hr

---

CASH IS COOL



ESTA BUSINESS CONFERENCE,  
EXHIBITION AND  
GENERAL ASSEMBLY

**ESTA**  
The Cash Management Companies Association

24 - 26 OCTOBER 2021, SEVILLA, SPAIN

# Content



1. Introduction
2. Changing landscape:  
*sleepwalking into cashless society?*
3. “Positive” aspects of cashless society
4. Perils: key takeaways

# 1. Introduction

- 2013; CNBC; Yahoo Finance; etc.
- even without and before covid-19, statistics showed the long-term trend of cash disappearing from the economic system
- larger context: global technological/financial giants, large commercial and central banks
- unbalanced discussion
  - denigration of cash

## 2. Changing landscape: *sleepwalking into cashless society?*



- a selection of cases:
  - Apple: new software that scans the entire device
  - Australia: app that combines facial recognition and location via satellites; military patrols, Orwellian laws enacted to eliminate cash
  - Facebook harvesting and reselling data
  - Google tracks payment history (Google Pay)
  - US administration's warrantless collection of citizens' personal financial data; credit information on 5 million consumers „for use in a wide range of policy research projects” (2013)
- ...further examples: Table 1.

## 2. Changing landscape: *sleepwalking into cashless society?*

Table 1. Examples of malfeasances with user data (1/3)

Publisher of the news*	Shortened link to the news	"Perpetrator/-s"	Exploit
Washington Journal of Law, Tech and Arts	<a href="https://tinyurl.com/yxqrjmul">tinyurl.com/yxqrjmul</a>	Amazon	Consumer generated mass surveillance
Business Insider	<a href="https://tinyurl.com/y3be8jk6">tinyurl.com/y3be8jk6</a>	Amazon	Spying/tracking users
Financial Times	<a href="https://tinyurl.com/y2yzzh2n">tinyurl.com/y2yzzh2n</a>	At least 34 apps (games, etc.)	Selling user data to Facebook
New York Times	<a href="https://tinyurl.com/y7lry8rw">tinyurl.com/y7lry8rw</a>	At least 75 companies	Spying/tracking users
Techcrunch	<a href="https://tinyurl.com/y9h3ky78">tinyurl.com/y9h3ky78</a>	Facebook	Spying/tracking users
35th Chaos Communication Congress	<a href="https://tinyurl.com/y3ja6w83">tinyurl.com/y3ja6w83</a>	Facebook	Tracking and selling user data even if user doesn't have FB account or app
Ars Technica	<a href="https://tinyurl.com/y3yby6ya">tinyurl.com/y3yby6ya</a>	Facebook	"Knowingly violated" privacy laws
The Verge	<a href="https://tinyurl.com/yckq85tt">tinyurl.com/yckq85tt</a>	Facebook	Spying/tracking users
Wired	<a href="https://tinyurl.com/y7o9muqb">tinyurl.com/y7o9muqb</a>	Facebook, Instagram, WhatsApp, Messenger	Sharing user data

Source: author

## 2. Changing landscape: *sleepwalking into cashless society?*

Table 1. Examples of malfeasances with user data (2/3)

Publisher of the news*	Shortened link to the news	"Perpetrator/-s"	Exploit
Business Insider	<a href="https://tinyurl.com/y7e9gbcm">tinyurl.com/y7e9gbcm</a>	Google	Creating "bubbles" by filtering search results
Deutsche Welle	<a href="https://tinyurl.com/yyazassz">tinyurl.com/yyazassz</a>	Google	Privacy breach
Techcrunch	<a href="https://tinyurl.com/yaopxlop">tinyurl.com/yaopxlop</a>	Google	Spying/tracking users
Medium	<a href="https://tinyurl.com/ydfmnbpe">tinyurl.com/ydfmnbpe</a>	Google	Spying/tracking users
Medium	<a href="https://tinyurl.com/yyjwzjh7">tinyurl.com/yyjwzjh7</a>	Google	Spying/tracking users
The Intercept	<a href="https://tinyurl.com/yagqxlh7">tinyurl.com/yagqxlh7</a>	Google	Spying/tracking users
Business Insider	<a href="https://tinyurl.com/y3jb37ac">tinyurl.com/y3jb37ac</a>	Google	Secretly putting microphones in devices
Search Engine Journal	<a href="https://tinyurl.com/y4uayhns">tinyurl.com/y4uayhns</a>	Google, Facebook, Twitter	Disrespecting the "Do Not Track" setting on web browsers
Bruce Schneier	<a href="https://tinyurl.com/y8yy9eh9">tinyurl.com/y8yy9eh9</a>	Government/-s	Placing surveillance cameras in streetlights
Wired	<a href="https://tinyurl.com/y7r24mel">tinyurl.com/y7r24mel</a>	Governments	Spying/tracking citizens
Fair	<a href="https://tinyurl.com/yyg47urs">tinyurl.com/yyg47urs</a>	Governments	Potential misuse of face recognition

Source: author

## 2. Changing landscape: *sleepwalking into cashless society?*

Table 1. Examples of malfeasances with user data (3/3)

Publisher of the news*	Shortened link to the news	"Perpetrator/-s"	Exploit
Motherboard	<a href="https://tinyurl.com/ya25y9wx">tinyurl.com/ya25y9wx</a>	Hundreds of free apps	Tracking and selling user data
Boingboing	<a href="https://tinyurl.com/yadvbxyv">tinyurl.com/yadvbxyv</a>	Lifx	Passwords saved insecurely (in a lightbulb)
Bloomberg	<a href="https://tinyurl.com/y9jzrjmf">tinyurl.com/y9jzrjmf</a>	Private DNA testing company	Leaking DNA data to FBI
Business Insider	<a href="https://tinyurl.com/ybjldmrg">tinyurl.com/ybjldmrg</a>	Smart TVs	Tracking and selling user data
Bleeping Computer	<a href="https://tinyurl.com/y49o9jr5">tinyurl.com/y49o9jr5</a>	Thousands of apps	Violating policies
Techcrunch	<a href="https://tinyurl.com/ycr4m3o5">tinyurl.com/ycr4m3o5</a>	Unknown	24 million financial and banking documents published online

Source: author



## 2. Changing landscape: *sleepwalking into cashless society?*

- big data mining
- detecting trends and patterns, modelling consumer behaviour
- we „choose” from what is pre-selected for us

...does it seem like freedom,  
or more like a *manipulation*?



### 3. “Positive” aspects of CS



- *fight against underground economy, illegal trading of weapons and drugs, trafficking, money laundering, tax evasion, and other black market activities*

...however,

- largest volume of the money laundering and tax evasion is performed by large banks and multinational corporations
- terrorism is mostly financed by certain sovereigns and intelligence agencies

### 3. “Positive” aspects of CS



- *cash is prone to stealing, security issues*

...however,

- credit cards are regularly stolen, web payments intercepted; never-ending records of online security breaches
- providing security in cash management is simple and inexpensive in comparison to providing security in a digital economy

### 3. “Positive” aspects of CS

- *cash is dirty, it carries bacteria and viruses*
- ...however,
- germs can be washed away with soap
- cash is immune to all known and yet to be imagined *digital* viruses, spyware, worms, trojans, and other malware
- regarding Covid-19; ECB:  
*„the risk of transmission via banknotes and coins is very low, and cash is safe to use”*

# 4. Perils: key takeaways

- the pursuit of anonymity: a natural longing for **privacy** and for basic **human respect**
- „*if you aren't doing anything wrong you have nothing to hide*” is an oversimplification of the conflict between the concepts of **control** and **liberty**
- the ultimate and the most powerful (material) tool/weapon/resource ever created by homo sapiens:  
**money in the hand**

# 4. Perils: key takeaways



- the fight for cash is more than it seems; it is a campaign for physical over virtual, for tangible over digital, for real over abstract, for human contact over cybernetic simulation.

**Fundamentally, it is a commitment to uphold individual power and liberty.**



**Thank you!**  
sajter@efos.hr

full paper available at:  
**[tiny.cc/ESTA2021](https://tiny.cc/ESTA2021)**

