# Computer Ethics in a Cyberwar Era

Wanbil W. Lee, President, The Computer Ethics Society

## Introduction

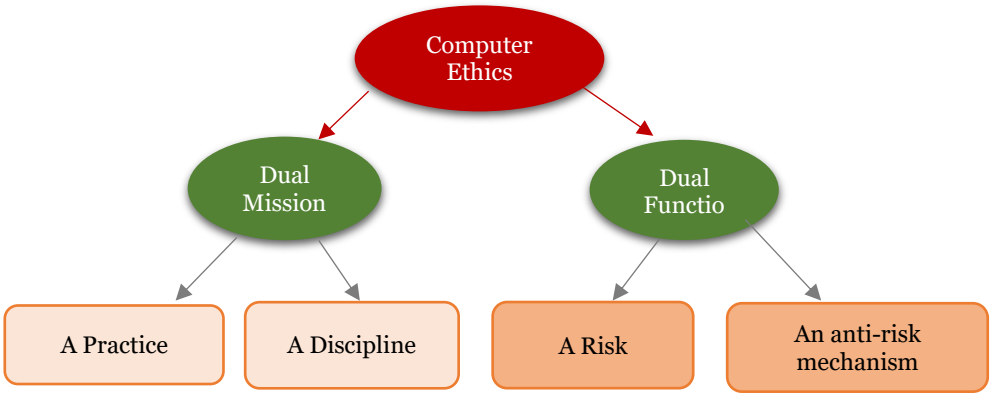
**We are entering a cyberwar era when we spend a lot on cybersecurity but still get hacked.** Why such a chronic and axiomatic phenomenon? The data protection strategy and apps are hitherto ineffective. Is it that simple? The attempt to respond argues strongly for taking cyberethics seriously and makes the point that data ethics/computer ethics is poised to lend a hand. The answer includes an explanation of some key issues that include definition and fallout of cyberwar, the big spending, the intersection of law and ethics and ethical issues, and a demonstration ethical analysis using a newly adapted application of Ethical matrix.

Data Ethics and Computer Ethics denotes more or less the same phenomenon, the former being a little trendy and the latter conservative.

**Data Ethics** is about the ethical issues involved in collecting, sharing, interpreting, synthesizing, and using data[1].

**Computer Ethics** is, in my view, a discipline cum practice grounded in ethical principles (Figure 1) that endeavours to promote and forward the highest professional and ethical standards in the work place, and to investigate the ethical impact of the extant theories and principles on the development and applications of the computer as well as the technological impact on the extant ethical principles, and to develop new theories/principles to fill gaps discovered in the investigation, if any[2] vis-à-vis a definition proposed by James Moore[3]. And this view is adopted by the Computer Ethics Society[4].

Figure 1 – Conceptual Graph of Computer Ethics




[1] Floridi, L & Taddeo, M (2016). "What is data ethics?" *Philosophical Transactions of the Royal Society A – Mathematical, Physical and Engineering Sciences, published 14 November 2016.DOI: 10.1098/rsta.2016.0360* (http://rsta.royalsocietypublishing.org/content/374/2083/20160360?utm_source=TrendMD&utm_medium=cpc&utm campaign=Philosophical_Transactions_A_TrendMD_0, Retrieved on 30 May 2017)

[2] Lee, W.W. (2014-15). Ethical, Legal & Social Issues. *Lecture Notes, Postgraduate Diploma in eHealth Informatics*, The University of Hong Kong

[3] Moore, J.H. (1985). "What is Computer Ethics?" in Johnson, D.B. & Nissenbaum, H. (Eds.) (1995), *Computers, Ethics & Social Values*, Prentice Hall, Upper Saddle River, NJ, pp. 7-15

[4] The Computer Ethics Society, http://www.iethicssoc.org

**Cyberwar:** Cyber espionage campaigns launched by hackers from one country targeting firms of another country result in the theft of business information such as bid prices, contracts and information related to mergers and acquisition – according to ComputerWorld[5]. The US-China trade-based and military-oriented cyberespionage some years ago; the crisis of Russian interference of the US general election in 2016; and the battle between UK and Russia over the tampering of Brexit voting are examples. The term is used in this context to include the battle between advertisers and users of ad blockers over "Blocking of Internet Advertising" (Ad blocking)[6].

**The big spending:** In recent years, security budges rise exponentially and amount to millions of US dollars. US Homeland Security reported that major financial institutions spent in 2016 US$1.5 billion on cybersecurity[7]. PWC reported that UK organizations doubled spending on information security: on average £6.2m in 2016 compared to £3m in 2015)[8]. According to a Forbes report, Gartner predicted worldwide spending on information security will reach $86.4 billion in 2017, and expected to grow to $93 billion in 2018[9]. These statistics and more are indeed worrying and consistent with the axiomatic "cyberattacks continue and damages increase big money spent notwithstanding, larger and larger.

Given the situation, probably without hesitation and by instinct, we point to the current data protection algorithms and blame it for being ineffective. The situation is exacerbated by the *new threats* that come with the rapidly advancing new technologies.

**(New) Threats/Crimes:** DX technologies (cloud, IoT, big data analytics, AI and machine learning) and new apps (Fintech, Medtech, etc) consume and create huge volume of sensitive data in multiple of locations, thus *putting the data subjects at risk*. According to ComputerWeekly, "nearly 70% of companies have their data breached this year [2018] and this rate is predicted to be growing every year". Ransomware attacks thousands of businesses with total damages up to billions of US dollars. WannaCry has hit computers from the UK's National Health Service where dozens of computers were infected every minute in mid-2017.[10] WannaMine, a new malware variant, took over computers around the world, hijacking them to mine a cryptocurrency called Monero early this year.[11] In a Hong Kong case reported on 15 May 2017, the ransomware encrypts the files of infected users, and demands payment of US$300 (HK$2,300) in bitcoins within three days for decryption. After the three-day deadline, the payment demand is raised to US$600 (HK$4,700) and after one week, all the files would be permanently encrypted.[12] Hence, *damages are more wide-ranging, severe and costly.*

---

[5] https://www.cw.com.hk/security/china-s-cyber-spies-hunt-for-business-information?mkt_tok=eyJpIjoiTXpnM1pUTXhaRGxpWm1NMSIsInQiOiJSU3IyOEd2bjhNcHZTWnVuMW96R1JlWFwvWkw1eHA1RStaMDkxUGdXUElOV1M5OFwvUmNoZXpncGREaG1CR3JqWlwvUXRcL2xkbzNESnkzdmYrV1I5NzRHTlNpQTNpVVVScm93amw5VytYSVwvaytNM0N5MzNqMmtYTFU1SFhcL2F5SHNiTSJ9&mrkid=23813682 Accessed 20 April 2018

[6] Wicker, SB and Karlsson, K (2017) "Internet Advertising: Technology, Ethics, and a Serious Difference of Opinion", *CACM*, Vol 60, No. 10, pp. 70-77

[7] US Homeland Security Research (2016) https://cdn2.hubspot.net/hubfs/533449/SecurityScorecard_2016_Financial_Report.pdf Retrieved 7 May 2017

[8] https://blog.cylonlab.com/increased-corporate-spending-on-cybersecurity-but-to-what-avail-1f8f46934b34 Accessed 18 April 2018

[9] Tony Bradley (17 August 2017) https://www.forbes.com/sites/tonybradley/2017/08/17/gartner-predicts-information-security-spending-to-reach-93-billion-in-2018/#650ca80e3e7f Retrieved 18 April 2018

[10] https://www.computerweekly.com/news/450419069/WannaCry-biggest-incident-to-date-for-National-Cyber-Security-Centre Accessed 22 April 2018

[11] https://www.pandasecurity.com/mediacenter/mobile-news/wannamine-cryptomining-malware/ Accessed 22 April 2018

[12] https://www.hongkongfp.com/2017/05/15/3-cases-wannacry-ransomware-virus-reported-hong-kong-far-says-official/ Accessed 22 April 2018

*Situation desperate!* So the new risks and soaring damages that are associated with the new threats render the existing anti-risk apps *dated* or *impotent*. However, data protection must go on even though it is becoming more challenging and expensive because data security is vital.

If left untouched, the status quo will continue to be grim: more new threats will be created to exploit the vulnerabilities, the already big spending will continue to escalate, the price for data protection will increase and the consumer will suffer. These issues are better left for the economists, lawyers, businessman, and even futurists. I suggest on this occasion to focus on the fundamental cause and possible remedy.

## Fundamental Cause & Remedy

A fundamental fault, I argue, is that the ethical impact in the design of data protection strategy and the formulation of information security policy has been given little or no consideration, and a possible way out is a change in design philosophy, to incorporate an ethical dimension in the decision space.

*Ethical Issues taken seriously*

Given that hacking or not hacking is by and large influenced by value judgment or sense of morality, and hacking is the major cyberwarfare. Deducing from this, ethical issues are a matter of course in cyberwar, and should be taken seriously. Indeed, there appear signs that cyber-ethical issues are gradually being taken seriously.

> The UK government, troubled with Big Data, established in 2016 its Data Ethics Council "as a means of addressing the growing legal and ethical challenges associated with balancing privacy, anonymization, security and public benefit", and the Hong Kong Privacy Commissioner proclaimed in his keynote speech at the GSMA Mobile World Congress in Barcelona, Spain in March this year that "Trust, Respect and Ethics in Managing Data are Crucial in Building a Better Future for Digital Economy".

*Ethical Issues Arising*

<u>Self-driving cars</u>

Tens of thousands of people die on the road and autonomous cars exacerbate the situation. The choice about who is going to be harmed and who's not is 'delegated' to the robot driver. That choice poses legal and ethical issues. In the event of an accident,

Where and with whom should the responsibility lie?
What right do the pedestrians, passengers, owners of the damaged properties, etc have?
Who should be prosecuted for the damages?

- The driver? But the driver is not a human. Is there law to sue a machine that is programmed to drive? Law always moves much more slowly than the event. So, there is no law yet.
- The human programmer? The programmer who merely carries out the job according to the specs, may be covered by the employer and shielded under the principle of deontology.

– The manufacturers of the autonomous car including the robot driver? The manufacturers tend to brush aside the associated moral issues.

Autonomous weapons

Like the episode with the self-driving cars, the situation here is akin to delegating the decision to a machine as who should live and who should die. The killer robot is programmed to "kill anything moving". It is difficult to tell an armed foe from an innocent civilian, to distinguish a soldier dressed as a civilian or a civilian dressed in uniform, etc. The "wrong guy" might be killed.

Who should be held responsible for the killer robots?
The politicians? The military user? The software company?
Or the engineers and scientists who design and implement the autonomous arsenal?

Criminal justice system

This is a set of risk assessment algorithms to judge a person's probability of re-committing a crime after having been released from prison. ProPublica reported that *systematic bias* was spotted by when carrying out an audit of this software[13]. Also unearthed was that the system makes mistakes about half the time, and underestimates the threat from white defendants while overestimates the threat from black defendants, resulting in white defendants being given leaner sentences, black defendants being given harsher sentences. When asked, the company that produced the algorithm said that it takes in something like 137 factors, but race is not one of them. Is AI to be blamed for the mistakes made in the criminal justice software?

The Uber hack

**Uber** revealed on 21 November 2017 that in late 2016, it found that potentially the personal information of 57 million Uber users and drivers were exposed, and paid the hackers $100,000 to keep silent about the hack and not alert those affected. It was further disclosed that it was not the hackers but GitHub, a service that Uber's engineers use to collaborate on software code that actually intruded into Uber's internal systems, the hackers downloaded the data stored on GitHub. Beware that convenience comes at cost and that a simple ride to the airport could potentially cost you your identity!

*Computer Ethics lending a hand*

**Ethical Computing** is the practice of Computer Ethics to address problems concerned with identifying/discovering ethical issues arising from developing and using computer-based application systems, analyzing these issues to come up with balanced solutions. The ethical

[13] https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing (2016) Accessed 23 April 2018

matrix method recently adapted [14] from food and agriculture[15] for IT, one of the tools for ethical analysis, is introduced and demonstrated in this presentation. The columns of the matrix correspond to "values" with respect to ethical principles, and the rows correspond to the stakeholders or interest groups. The number of columns and rows varies as required.

*Blocking of Internet Advertising*

Internet advertising attracts viewers because of the content it provides free. It attracts the advertisers because it is incredibly effective at targeting specific viewers. [For example, a seller of waterproof speakers might want to target those in the 16 to 40 age bracket interested in swimming, boating, or water sports.] It can be a platform for the content generators and publishers to make a revenue. Since it allows anyone to advertise with little transparency, the platform can also easily abused for nefarious purposes, for example, a bug in Facebook made it possible for potential hackers to uncover ad users' personal data. Therefore, ad blocking emerges.

Ad blocking amounts to a war between ad lovers and ad blockers, with the neutral group playing onlookers. The impact of war can be: users of ad blockers enjoy freedom of the "annoying" advertisements; content developers and publishers suffer a reduction in income; advertisers may turn to other venues; some content generators may discontinue business; some publishers may produce lower quality content so that the ad viewing users will be badly off.

Is blocking of Internet Advertising (Ad blocking) unlawful and unethical? (A first-cut result of ethical analysis using the Ethical Matrix method is shown in Figure3 below.)

Figure 3 – A First-cut Result

| Values / Stakeholder | Well-being (utilitarian/consequential) | Deontic Ethics | Virtue Ethics | Justice/Fairness |
|---|---|---|---|---|
| **Ad blocking users** | **Ethical – happy with reduced free ads** | **Unethical** | **Ethical – self-defence** | **lawful** |
| **Ad Content generators/publishers** | **Unhappy – receive a lesser revenue** | **Ethical** | **Unethical – design unethical** | **Income lowered** |
| Ad viewing users | Unhappy | | | less and lower quality ads |
| Advertisers | Unhappy | Ethical | | Fewer choice of avenue for ad |
| Internet users indifferent to ads | May be less 'informed' because of less free ads | | | Not affected |

[14] Lee, W.W. (2014). Why Computer Ethics Matters to Computer Auditing. *ISACA Journal*, 2, pp. 48-52 or
Lee, W.W. (2017). Ethical Computing continues from Problem to Solution. In M. Khosrow-Pour (Ed.), *Encyclopedia of Information Science and Technology* (4th ed.; pp. 4884–4897)
[15] Mepham, B., Kaiser, M., Thorstensen, E., Tomkins, S., & Millar, K. (2006). *Ethical Matrix Manual*. The Hague: LEI http://www.ethicaltools.info/content/ ET2 Manual EM (Binnenwerk 45p).pdf

Ad blocking could breach contract (implicit contract) which is assumed between the providers of the content (advertisement) and the viewers (of the free ads), where implicit contract requires a show of an unambiguous offer and unambiguous acceptance. However, since not all internet users are happy to see the massive free ads or there may be a large number of consumers feeling frightened by the spyware and malwares that were embedded in those ads without notice, there can be no unambiguous offer (to the viewers) and no unambiguous acceptance (by the viewers). Therefore, implicit contact does not exist (in the US anyway) and blocking Internet Advertisement *is lawful*.

But ad blocking could be ethical or unethical. Taking the view of the welfare for the ad blocking users on ground of utility or consequence, *it is ethical*; taking the view of *rights* of the content providers (generators, publishers and advertisers) on ground of duty and virtue, *it is unethical*. [Note: *rights* refer to the right to enjoy the return for the investment by the providers (the content generators and publishers, and advertisers) – US$22 billion in 2015 was reported, and the right to enjoy the free ads by the Internet users in general, and *welfare* means enjoyment of freedom from the unwanted advertisements by the ad blocking users].

Ad blocking affects a whole host of interested parties: the ad blocking users, the ad viewers, the free content providers (generators and publishers), and the advertisers.

- Ad blocking apps users will be happier [as a result of a reduced amount of the unwanted ads]
- Content generators and publishers will be unhappy [because they will in general receive a lesser revenue.]
- Ad viewers are unhappy [because some of the content generators and publishers will have to reduce or stop the provision of content or produce a lower quality content.]
- Advertisers may have fewer choices and suffer the trouble of looking for and shifting to alternative venues, but will not be significantly affected [though this will further reduce the income of the content generators and publishers.]
- Indifferent Onlookers (Internet users who are indifferent (to ad blocking) or may or may not turn away from the free content), may have less free ads.

<u>Analysis based on utilitarian ethics</u>

From a utility (or well-being) view, and assuming that the decision made by ad blocking users is rational and that the number of Internet users at large significantly exceeds the number of ad content providers (generators and publishers), the use of ad blockers provides the greatest happiness for the greatest number of people. [Note: Utilitarianism holds that "an act is morally right if that act maximizes utility or brings about the largest amount of happiness or well-being to, and reduces suffering of the greatest number of people".] **Ad blocking is ethical.**

<u>Analysis based on deontic ethics</u>

This conclusion would certainly not please the content generators and publishers. Indeed, utilitarianism or consequentialism does not take into consideration of all stakeholders, and a

deontic reasoning returns an opposite conclusion. The ad blocking users treat the content providers as a means rather than an end; they exploit the content without paying respect to the efforts which the providers created for a living. So, ad blocking violates the Kantian *categorical imperative* (which states "Treat people as an end; never only as a means to an end"). Also, ad blocking breaks the Golden Rule (which says ("Do unto others as you would have them do unto you" or "We should do to others what we would want others to do to us"). **Ad blocking or the use of ad blocking is unethical**.

Virtue Ethics

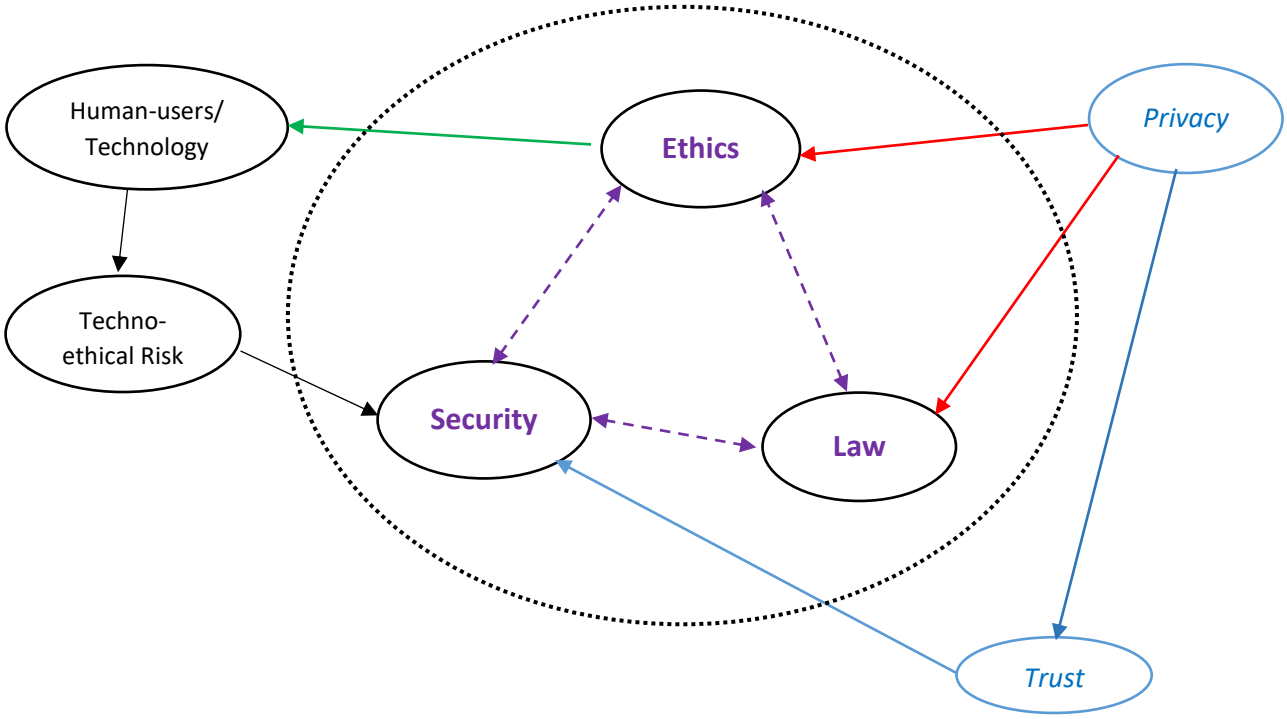
Virtue Ethicists advise us to live according the values we cherish and care. Applying this view onto ad blocking (which is the product of a technical design which should embed knowledge, freedom and autonomy that are prerequisites for our growth), and measuring against value-based design practices which capture various fundamental human values, **the design of the internet advertising is unethical** but the use of ad blocking as a matter of self-defence is ethical. What this may mean for us is a virtue-based design carried out under an *informed, unforced agreement* that acceptable to all stakeholders.

## Takeaway

1. Take ethical issues seriously.
2. Know your common ethical principles:
   Act to bring maximum happiness to maximum number of people – *consequentialism/utilitarianism*
   Act to be fair; treat others as an end, never only as a means to an end – *Kantianism/deontology*
   Don't do to others what we don't want them to do to us – *Golden Rule*
   Live according to the values cherished and cared by us all – *Virtue Ethics*
   But note that sometimes these principles may be in conflict – Ad Blocking is a case in point. Self-reflection and self-disciplined helps in making a balanced decision. The Ethical Matrix is a new approach to ethical analysis.
3. Remember, *Ethics is a risk, too.*
   Violating ethical principles when using the computer is a risk. When realized, that risk cyberbullying: reputation-distortion, falsification of identity, and the like will lead to crime.
4. Also, *Ethics, Law and Security are linked.*
   Ethics and law seem separate, yet linked. In the Donald Tsang case [noting that Tsang was a former Chief Executive of the HKSAR], the judge instructed the jury: "This is a legal case, not a moral case." – *Law and ethics seem separate*. The defence counsel pleaded for a suspended sentence and a shorter term, relying on "lack of morally questionable motive" in this case: "Heavier sentence if motives morally questionable". (South China Morning Post, 2017b) – *Law and ethics appear interrelated*.
   Security, ethics and law are linked (Figure 3). Abuse of the technology (by human-users) is a risk (a techno-ethical risk) as it violates ethics as alluded to earlier; certainly a security concern. Trust depends on security: No trust, no security since no one will trust you if you act in contradiction to ethics or fail to obey the rule of law. [A case in point: Zuckerberg's seemingly courageous response (admitting mistakes and

apologizing) in the grilling sessions in the US congress recently may have won him trust and a contributing factor to Facebook's stock performance (a rise in stock price)[16]].

Figure 3 – Security-Ethics-Law




[16] *ComputerWeekly* (contributed by Warwick Ashford) Facebook posts strong first quarter despite privacy scandal https://www.computerweekly.com/news/252439971/Facebook-posts-strong-first-quarter-despite-privacy-scandal?asrc=EM_EDA_94107517&utm_medium=EM&utm_source=EDA&utm_campaign=20180427_Facebook%20posts%20strong%20first%20quarter%20despite%20privacy%20scandal (26 April 2018) Accessed 28 April 2018