

Introduction to Digital Media

The Digital Media & Politics

DGM 711

Lecture 9

Prepared by

Dr. Shereen Kedwany

Reminder



- **The public sphere**, is a fundamental component of modern **democracies**, where **individuals** are **free** to **discuss politics** without being subject to an external **authority**, and can thus form a **public opinion**.
- **Media publics** can successfully become **politically active** thanks to the emergence of an **information-rich digital environment** and its related **communication tools**.
- **Digital technologies** also favored the emergence of **new kinds of players** in the contemporary **public sphere**, such as **WikiLeaks** and **Panama papers**.
- **The networked public sphere** is not inherently **democratic** in nature.
- The **algorithms** that underpin digital platforms shape **political and social interactions**.
- These are new forms of “**algorithmic gatekeeping**,”



- I. The Digital Divide .
- II. The Political Activity & Digital Media .
- III. The Digital Surveillance .
- IV. Conclusion.

- **Power relations** are now systematically organized around **digital media**, the ability to determine who can **access** them, as well as the planning and management of **information flows**.
- This phenomenon has been transformed and strengthened by the emergence of the **networked public sphere**, but was present before the mass diffusion of digital media.

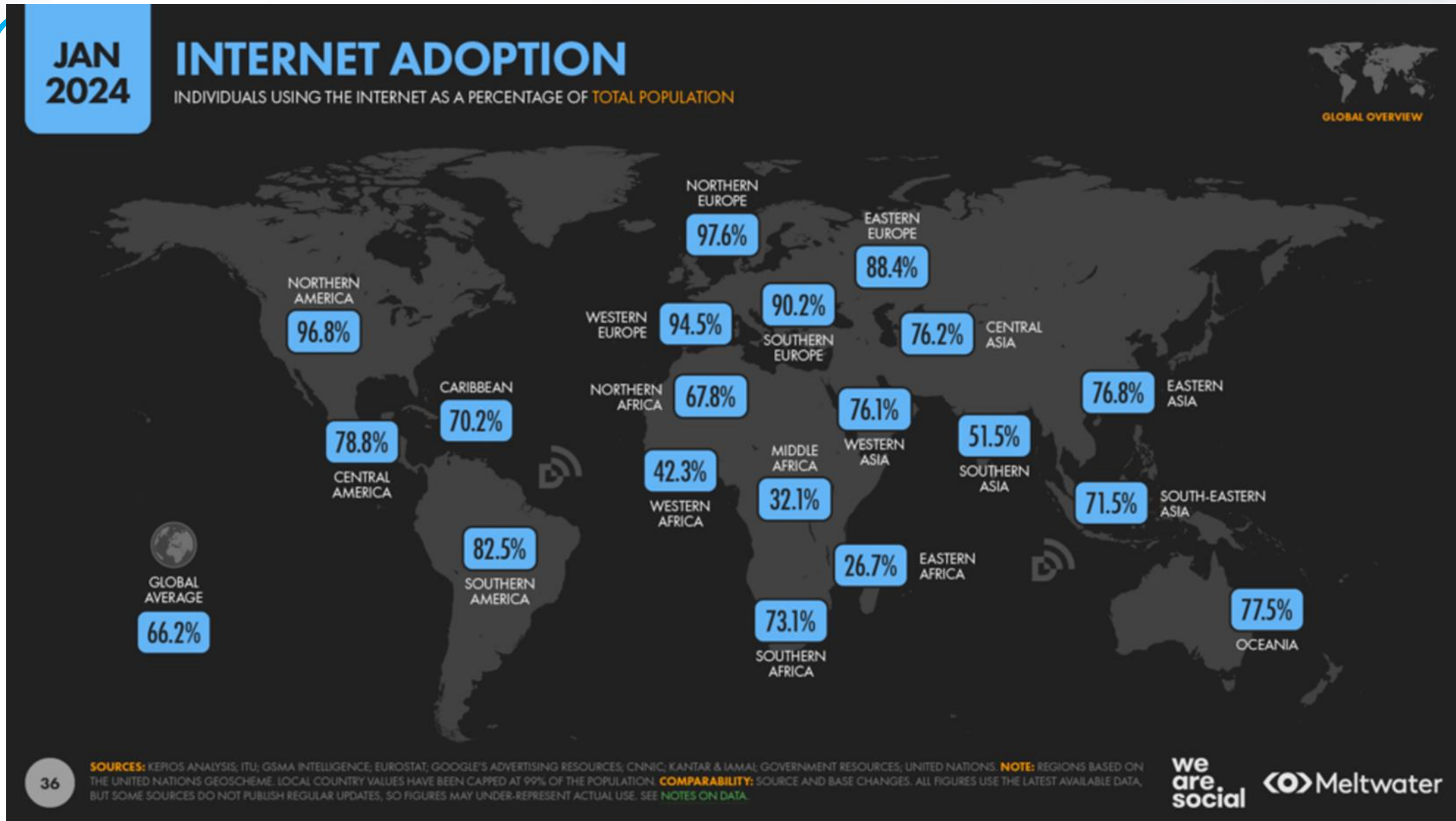


- Since the **1990s** there has been an **increase** in the number of **citizens** who **access information and participate in political debates through digital media**, while the number of individuals using only **other media** such as newspapers, radio, or television has **decreased**.
- This **change** is gradual and develops **unevenly** in **different areas** of the world and social groups.
- Indeed, although the internet can broaden **citizen participation** in the **public sphere**, access to **digital technologies** is **uneven**.



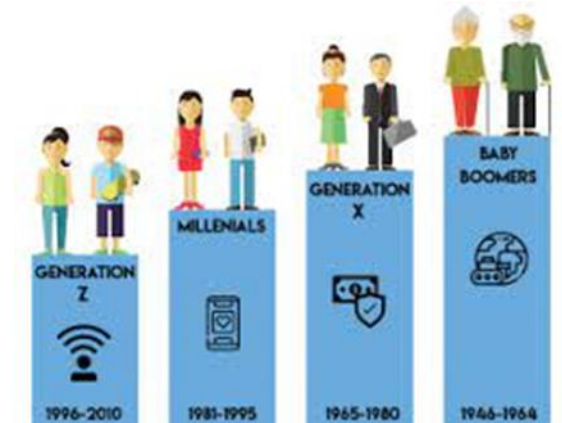
- With the definition **digital divide**, media theorists highlighted the **difference in access to network technologies** that occurs **between rich countries and poor countries**, or between different **classes or generations** within the same country .
- Indeed, in most **advanced economies** access to **digital technologies** and services is significantly higher than in **developing countries** .





- **Source:** <https://wearesocial.com/uk/blog/2024/01/digital-2024/>

- Furthermore, within a certain area the **elderly, women, and low-income** communities may experience a **digital divide** in relation to **other social groups**.
- Yet these **divides** tend to be the result of a multiplicity of **factors**.
- For example, research on **Seniors** has confirmed the existence of both a “**generational gap**” and intergenerational differences in the use of mobile technologies such as tablets and mobile phones.



- Such **divides** depend on several **technological and socio-economic factors** and cannot be reduced to age alone .
- The effects of these changes also depend on **the type of society** in which they occur.
- **Policies** related to **access to and transparency of information** contribute to shaping how **power** is distributed.
- **Governments** pursue initiatives to **control access to information**, and often are reluctant to foster greater **transparency**.



- In **authoritarian countries** the distributed architecture of **digital networks** can make the **control** of **information flows**, and therefore of **the public sphere**, more **difficult**.
- This difficulty can create room for free speech, as actors such as **social movements** may be able to use **digital media** to communicate freely in contexts in which the **public sphere** is strictly **controlled by a regime**.



- On the other hand, these very changes can also give **authoritarian regimes** new tools to **control** the population, since activities on **digital media** are **easily traceable** and **subject to surveillance**.
- Fears of a **less controllable public sphere** have led some **governments**, for example in **North Korea**, to **restrict access to some digital services** within the country.
- This can have repercussions not only on **freedom of speech**, but also on **economic development**.



- **Non-democratic governments**, such as **China's**, tend to exercise a very tight **control on information flows**.
- The **Chinese government** filters unwanted content through its “**Great Firewall of China**,” a set of **algorithms** and other technologies that select sources and prevent the passage of certain types of information.
- **Users** of that country's internet are denied access to a number of **websites** and online resources, for example **newspapers** that publish information **against the government**.



- some of these problems exist in many **democratic countries**, which may resort to **censorship, filters**, or other measures that **restrict freedom of expression through digital media**.
- In sum, **freedom of expression** and the **right to access information** cannot be taken for granted, but rather need continuous revisions and **negotiations**, and are at the center of frequent **legal and political battles** .
- As a response, some **countries** have discussed and implemented initiatives to protect **freedom of expression and transparency**.



- Through a series of **laws** developed in the **2010s**, **Iceland** has set the goal of becoming a **safe haven** that protects journalists, internet users, and publishers around the world, while at the same time imposing increased transparency to the government.
- These **laws** also aim to attract publishers, databases, and internet providers to the **Icelandic market**.



- **Political activity** is profoundly influenced by the **media**, as well as by **information management systems**.
- If the most optimistic trends saw the **networked public sphere** as a means of creating forms of **direct democracy** intended to supplant the **institutions of representative democracy**, other more pessimistic accounts tend to see it as a **reinforcement of existing hierarchies**.
- It is probably more correct to say that **digital networks** make new and different strategies of **mobilization and participation** possible, while at the same time providing an even greater **power** to some **political actors**.



- In **Western societies**, many **political practices** significantly depend on the ability to **analyze the electorate** with **techniques** in order to produce **political marketing strategies targeted** at different **media**.
- **Political parties** develop **platforms** to collect **data** on their **voters** and **supporters**, collect **donations**, and communicate **political content**.



- In the **United States**, both the **Democratic and the Republican Party** run massive **databases** containing information about tens of millions of potential voters, such as data on demographic characteristics, voting behavior, and even purchasing behavior .
- These **data** allow analysts to assign an **individual profile to potential voters** and arrange **direct information flows** through **techniques** borrowed from **commercial marketing**.
- In the early **2000s** for example **the Republican database, Voter Vault**, was much broader and more detailed than that of **the Democratic Party**.
- This was one of the ingredients of **George W. Bush's** success in the presidential elections of 2000 and 2004.



- **Barack Obama's** race for the primaries of the **Democratic Party** and subsequent victory in the **US presidential elections** in **2008** is an example of the use of forms of **digital- based collaboration for political purposes**, as principles of grassroots political organizing were applied to the digital environment.
- Thanks to a **campaign** based mainly on **online platforms** and created with the fundamental contribution of important figures in the world of digital media, like **Chris Hughes, co-founder of Facebook**, who was responsible for his **online campaign**, **Obama** was able to defeat opponents in terms of number of people directly involved in his **campaign**, **funds** raised and, finally, **votes**.



- Although the practices put in place by **Obama** cannot be considered the sole reason for his victory, his strategy leaving his supporters free to act and coordinate autonomously, but maintaining centralized control, has been studied as an early example of the **political potential of digital environments**.
- The **my.barackobama.com** site played a crucial role, with **15 million Members** who used it to organize at the local level for **campaigning** and fundraising (Castells 2009).



- In the same electoral cycle, **Donald Trump** was backed by an array of right-wing groups that used websites such as **4chan** (an underground imageboard forum) to produce and distribute **memes** and other **viral content** that increased the popularity of Trump or attacked Clinton, his opponent (Goerzen 2017).
- In both cases, these initiatives **mobilized** hundreds of thousands of people, more than those involved in the **official campaigns**.



- In **Europe**, new **political parties** have adopted not only **communication** but also **organizing strategies** based on **digital networks**.
- In **2017** in the **United Kingdom**, supporters of the **Labour Party** leader **Jeremy Corbyn** developed a **smartphone app** to coordinate delegates during the party's conference .
- In **Italy**, the **Five Star Movement** uses its **digital platforms** to create a space in which people with different **political backgrounds** converge to openly **discuss** issues of interest and **vote** on candidates and proposals.



- Other examples are **Podemos** in the **Spanish state** or the **Pirate Party** in **Iceland**, a **political movement** led by an interest in transparency and freedom of expression, the protection of individual digital rights and privacy, and intellectual property law reform.
- These **parties** have grown to become major **political actors**, elected representatives in national legislations and at the **European Parliament**.
- They promote **digital-media**-based forms of **political participation**.



- These “**digital parties**” may signal the emergence of organizational structures that in the future could ensure a vibrant and dynamic **democratic debate** attuned to the **networked public sphere**, while representing an **alternative** to the **traditional mass parties** of the twentieth century .
- Some authors argue that these forms of **digital democracy** arise from the success of institutions like **Wikipedia**, which are based on a **culture of participation** based on **direct access to information** and online cooperation (Tkacz 2015).



- On the other hand, **digital media** provide new tools for **social control and repression**.
- Indeed, **digital networks** are characterized by a state of “**passive participation**” in which most **information** is not in the hands of the **individuals** who generated it but rather used by other **actors** and for purposes **outside of user control**.
- **Individuals** are **passively** subject to this **power**, regardless of their political intentions and expectations .



- Any **activity** on **digital media**, whether it is **access** to a website, **search** engine use, **interaction** on social media, or **exchange** of messages via smartphone, leaves **traces** that are **collected** and **monitored**.
- **User data** are in fact **recorded**, **analyzed**, and used for purposes of **social control** or **profit**.
- This form of **passive participation** is created by **two** distinct but interlinked **processes**:



- **1- Data capture** is a set of processes that use information extracted from the analysis of **user behavior** and interaction to increase the **efficiency of web companies** (Agre 1994).
- For example, **Google** uses **user data** – from your **communications** via **Gmail** and **Google searches**, to your movements tracked through **Android phones** – to create **consumer profiles** and then uses them to present **personalized advertising** to individual **users**.



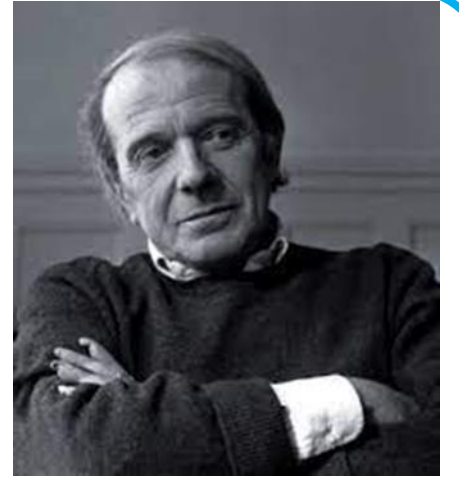
- 2- Surveillance is a process of data collection and analysis undertaken by public or private actors in order to control the behavior of individuals.
- In many cases, **governments** use **agreements** with **web corporations** to access **data** on their citizens.
- While **corporate data capture** allows the modification and improvement of the **user experience**, **surveillance** is **covert** and not perceptible by the **user**.



- In the **1970s**, French historian and philosopher **Michel Foucault** described the birth of a “**disciplinary society**” characterized by the pervasiveness of institutions dedicated to **observing and normalizing citizens' behavior** (1977).
- To describe **disciplinary power**, **Foucault** used the example of the **Panopticon**, a **prison** designed in the eighteenth century by the English philosopher and jurist **Jeremy Bentham**.
- The **architecture** of this building allows **one person to control** all the **prisoners**, who are always **visible** but are not able to tell whether they are being observed.



- Similarly, the **modern disciplinary society** analyzed by **Foucault** was based on **institutional control** over individuals.
- Another French philosopher, **Gilles Deleuze**, has proposed that the contemporary era is characterized by the transition to a “**society of control**” in which **power** is exercised through continuous and instantaneous control of the population, and even spread in the “**brains and bodies**” of the **citizens** (1992).



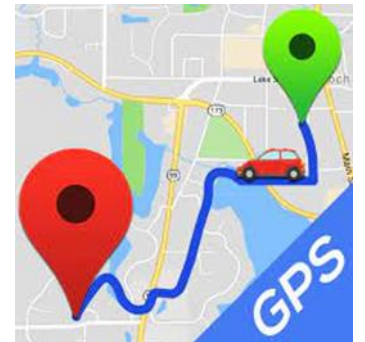
- Several authors have referred to Foucault and Deleuze in order to interpret **surveillance** processes carried out through **digital technologies**, in particular since the **2010s** and, later on, in reaction to revelations about the depth and reach of today's **surveillance systems**.
- In **2013**, the American computer programmer **Edward Snowden** revealed to the world the existence of **secret spying programs** put in place by the **National Security Agency (NSA)**, a US government agency.



- Thanks to Snowden's revelations, as well as further information that emerged later, we know that several **Western governments**, particularly the **US**, operate **surveillance systems** that allow them to **record all phone and online interactions**.
- These **systems** are often used without the mandate of a **court** (Greenwald 2014).



- **Surveillance** processes depend on the cooperation of large **web corporations**, which have **access to the data generated by users** and capture it to **improve their services** or provide **personalized advertising**.
- Thanks to this collaboration, **state agencies** can, for example, turn on the **camera and microphone of any laptop or smartphone** and use them to **spy** on a person without their knowledge.
- These **agencies** have created **databases** that contain information on all **digital communications**, and in some cases have **access to data** about the movements of users of **mobile phones** with **GPS**.



- Thanks to **algorithms** that analyze the collected data, both **web companies** and **surveillance agencies** can construct the “**profile**” of a **user**, that is, a statistical extrapolation used to recognize and interpret patterns of **behavior**.
- This is the result of **corporations**’ reliance on data capture and analytics as a core part of their **business model**.



- In **2018**, further revelations about the intertwining of **political surveillance** and **social media commercial interests** surfaced.
- The **Guardian** released the so-called **Cambridge Analytica Files**, a set of information revealing that **Facebook** had sold **data** from millions of unknowing users to a **company** that used them to influence the **2016 US elections** (Cadwalladr 2018).



- The ability of **corporations** such as **Google** or **Facebook** to extract relevant **data** from any **human behavior** has prompted social theorists to use definitions such as “**surveillance capitalism**” to describe the **economic systems** that sustain surveillance (Zuboff 2016).



- On the other hand, **surveillance** is presented by **governments** as a **useful** practice aimed at **protecting society** from criminal or terrorist activities.
- However, **digital technologies** have expanded **surveillance** to the entire population, in a sense making concrete **the society of control** imagined by **Deleuze**.
- The **collection** of masses of **data** from **surveillance** cameras, emails, social media, web browsing, and phone calls is no longer targeted at individual suspects, but rather extended to **all citizens**.



- Conversely, **resistance to surveillance** is based on **technologies and actions** that allow users to not produce data, or to make them **untraceable** or not analyzable .
- The growing **awareness** of the pervasiveness of surveillance in digital environments has fostered forms of **resistance**.
- While **stricter regulation** remains the most important way to defend digital media users from **privacy** breaches, **individuals** can choose specific **strategies** to **resist surveillance**.
- Some are **technical**.



- **Encryption** is based on a set of **coding techniques** that allow a user to read a text only if they possess its key.
- One of the most used technologies for the exchange of **encrypted emails** is **PGP (Pretty Good Privacy)**, an **encryption system** in which two **users** exchange deciphering keys that are generated for each message and thus are relatively **secure**.



- Other **strategies** are **political** and have to do with **individual** and **collective** choices.
- **Refusal**, that is choosing not to participate in the activities underpinned by commercial web services, may also be a form of **resistance to surveillance** and other forms of uneven power.
- In some cases, the decision to abandon a dominant **social media** platform such as Facebook may be a way to assert one's individuality as a consumer rather than a politically oriented decision (Portwood-Stacer 2012).



- Indeed, the **refusal to participate** is a known **commercial problem** for **social media business models**; sites such as Facebook need to protect themselves by, for example, designing more engaging user relations .
- Finally, in societies in which the **public sphere** is highly dependent on **digital platforms**, and **social media use** is considered a prerequisite to a meaningful **political life**, forms of **media refusal** that are not followed by the construction of **alternatives**, such as so-called “**Facebook suicides**,” may result in **marginalization** .



Conclusion



- **Power relations** are now systematically organized around **digital media** and the **networked public sphere**
- There has been an **increase** in the number of **citizens** who **access information** and **participate in political debates through digital media**.
- **Digital divide** is the **difference in access to network technologies** that occurs **between rich countries and poor countries**, which depends on **the type of society Policies** related to **access to and transparency of information** .
- Several **Western governments** operate **surveillance systems** that allow them to **record all phone and online interactions**.
- **Web corporations** capture **users' data** to **improve their services** or provide **personalized advertising**.
- **Individuals** can choose specific **strategies** to **resist surveillance**, such as **encryption** or **refusal** of participation in the commercial web services



Thank You